GESTÃO DA SEGURANÇA DA INFORMAÇÃO

INTRODUÇÃO

Curso Superior de Tecnologia em Segurança da Informação e Gestão da Tecnologia da Informação

Prof. Nasser Arabi
Com adaptações: Clenio Emidio

Desafios atuais

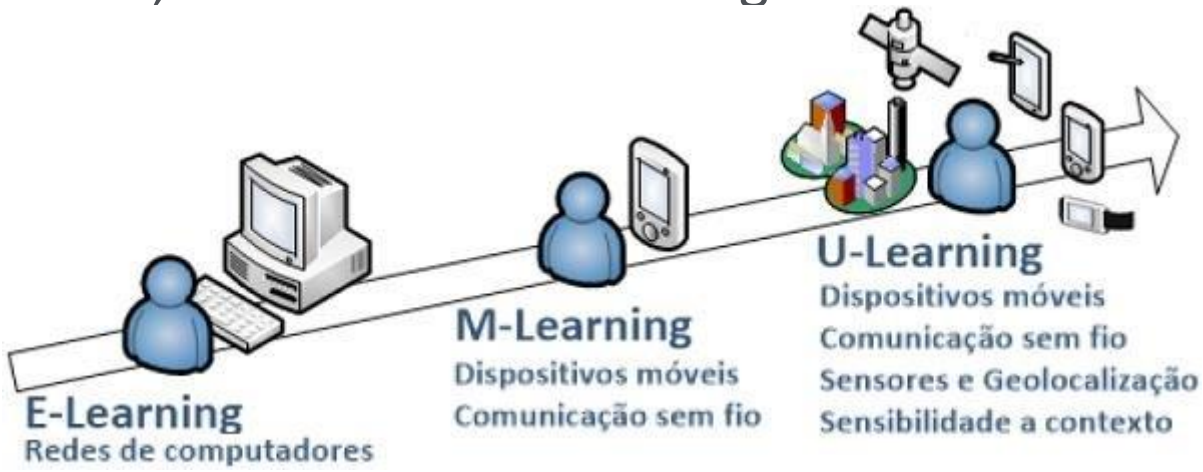
Com a evolução das ameaças cibernéticas, a segurança da informação enfrenta ataques sofisticados, vazamentos de dados e engenharia social.

Papel de todos: A segurança da informação é uma responsabilidade compartilhada por indivíduos, empresas e governos. A educação e a conscientização são cruciais para proteger a si mesmo e aos outros.

Somente a TI é culpada?

A importância da Segurança da Informação no mundo digital Atual

A informação é um ativo valioso e a conectividade digital se tornou ubíqua.
u-learning
A revolução tecnológica trouxe inúmeras vantagens, mas também desafios significativos relacionados à segurança da informação.
Neste cenário, entender e aplicar conceitos de segurança tornou-se essencial para proteger nossa privacidade, identidade e ativos digitais.



* Estar em toda parte

Segurança no mundo digital Atual

Explosão Digital: estamos rodeados por ativos conectados, desde smartphones até dispositivos de cada inteligente e sistemas de controle industrial. A quantidade de dados gerados e compartilhados cresce exponencialmente a cada dia.
Riscos emergentes: A crescente interconexão também traz riscos emergentes, como ciberataques direcionados, roubo de dados pessoais e empresariais, espionagem cibernética e vandalismo digital.

O que não se pode esquecer

Privacidade ameaçada: Nossas informações são valiosas para criminosos cibernéticos. A Falta de segurança pode resultar até em extorsão.
Impacto nos Negócios: Para as organizações, a segurança da informação tornou-se uma questão crítica. Uma violação de dados pode prejudicar a reputação, resultar em perdas financeiras e desencadear implicações legais.
Desafios globais: Desafio global que afeta empresas, gove e indivíduos em todos os lugares. Ações coordenadas são necessárias para combater ameaças cibernéticas transfronteiriças.
Educação e conscientização: a conscientização e o conhecimento são a primeira linha de defesa. Ao compreende as ameaças e adotar práticas seguras, podemos reduzir nossa vulnerabilidade.

Conceito de Segurança da Informação

É a proteção dos sistemas de informação contra a negação de serviço a usuários autorizados, assim como contra a intrusão, e a modificação não-autorizada de dados ou informações, armazenados, em processamento ou em trânsito, abrangendo 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 (NBR 17999*, 2003)

NBR – Normas Técnicas Brasileiras / ABNT

* Atualizada por meio da ISO/IEC 27002

ISO - International Organization for Standardization

- Instituição cujo objetivo é propor e monitorar normas que representem e traduzam o consenso de diferentes países para a normalização de procedimentos, medidas e materiais em todos os domínios da atividade produtiva.

ABNT - Associação Brasileira de Normas Técnicas

- Sociedade privada sem fins lucrativos, fundada em 1940 para fornecer a base necessária ao desenvolvimento tecnológico brasileiro e é o órgão responsável pela normalização técnica no país.
- Grupos participam dos mais variados temas.
- CB-21 (Computadores e Processamento de Dados): computadores e processamento de dados, automação em geral, controle de acesso 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,

Segurança da Informação segundo a NBR ISO/IEC 27002

Fonte: webaula Estácio

Sistemas de informação

... é um conjunto organizado de pessoas, hardware, software, rede de comunicação e dados, que são coletados e transformados em informação dentro de um ambiente organizacional. (O'BRIEN 2004)

... seja ele um sistema informacional computadorizado, seja manual... (wikipedia)

http://rmfais.com/

O papel estratégico dos sistemas de informação

Fonte: webaula Estácio

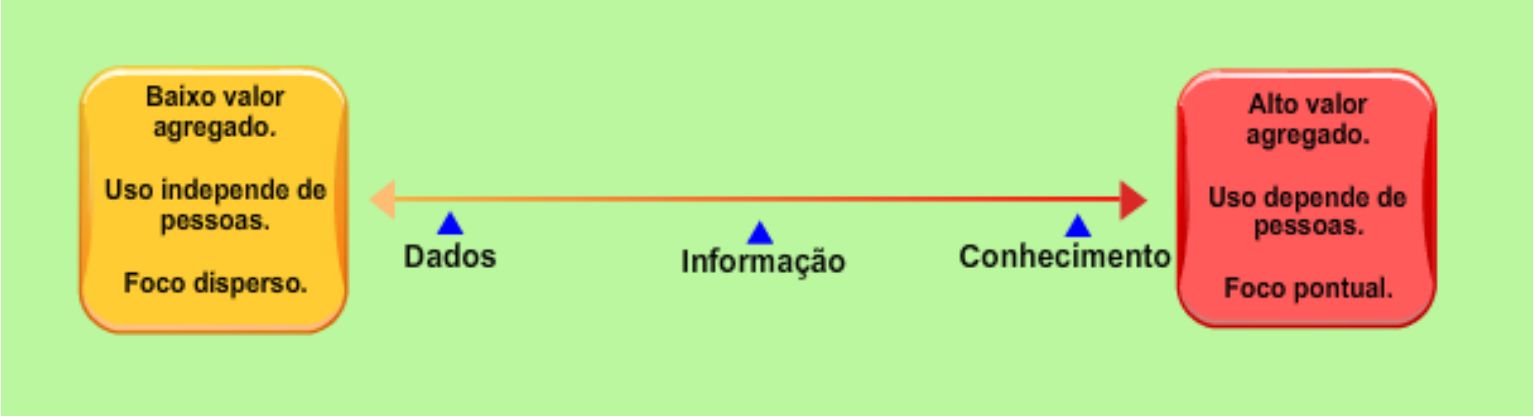
O que é Informação

Dados	É a coleta de matéria-prima bruta, dispersa nos documentos
Informação	É o tratamento do dado, transformado em Informação. Pressupõe uma estrutura de dados organizada e formal. As bases e bancos de dados, bem como as redes são sustentadas pela informação.
Conhecimento	É o conteúdo informacional contido nos documentos, nas várias fontes de informação e na bagagem pessoal de cada indivíduo.
Inteligência	É combinação destes três elementos resultante do processo de análise e validação por especialista. É a informação com valor agregado. Fonte: Stollenwerker – Petrobrás 1997

Fonte: webaula Estácio

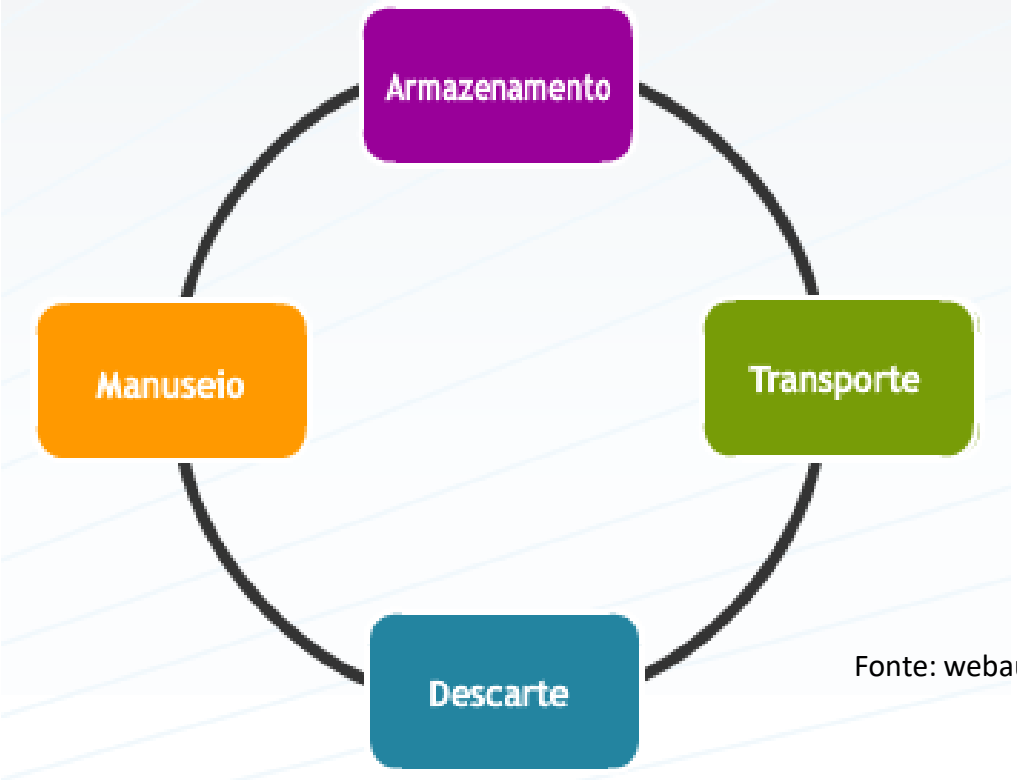
O propósito da Informação...

O **propósito da informação** é o de possibilitar o alcance de objetivos pelo uso eficiente dos recursos disponíveis (pessoas, materiais, equipamentos, tecnologia, dinheiro e informação).



Fonte: webaula Estácio

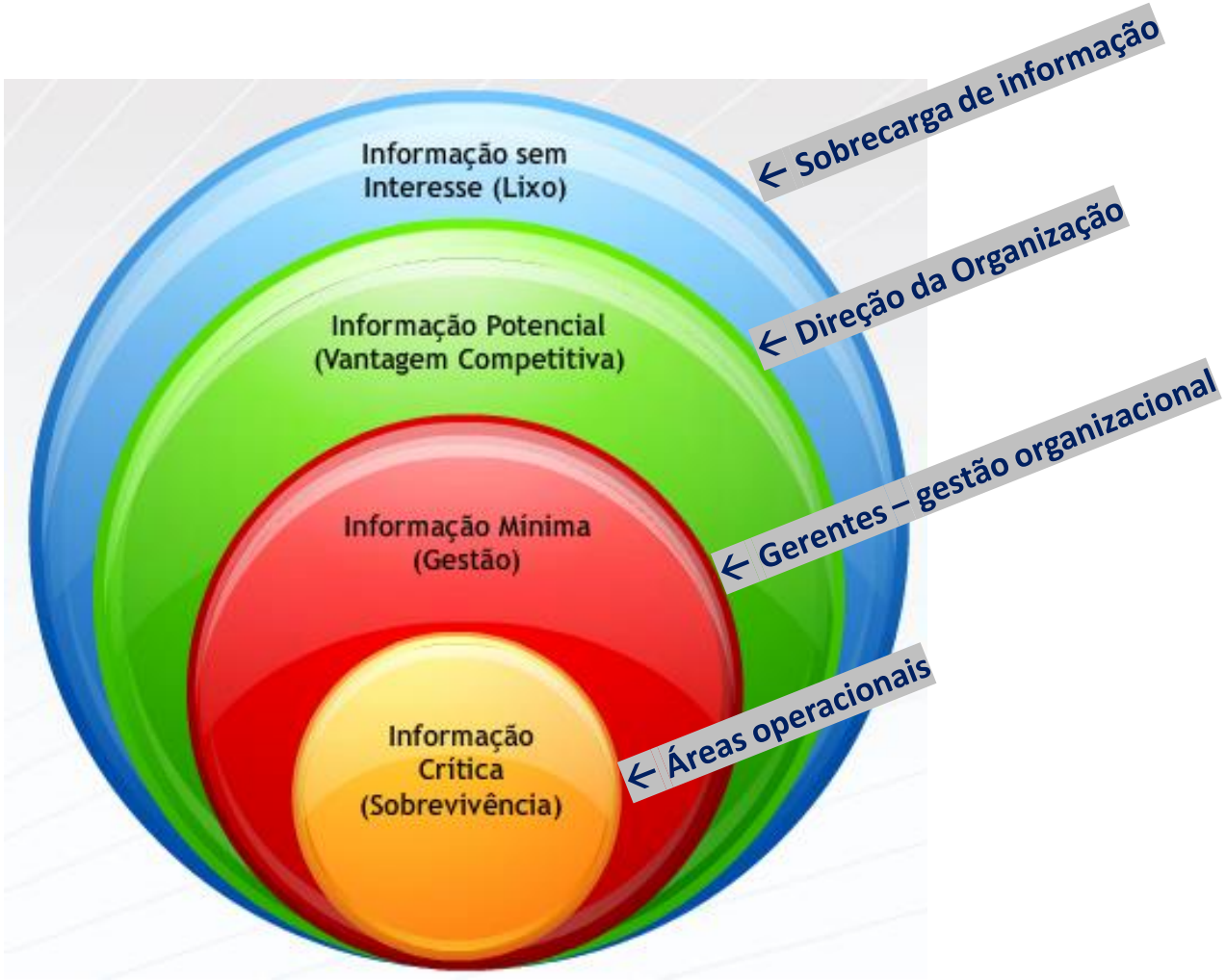
Ciclo de vida da Informação



Fonte: webaula Estácio

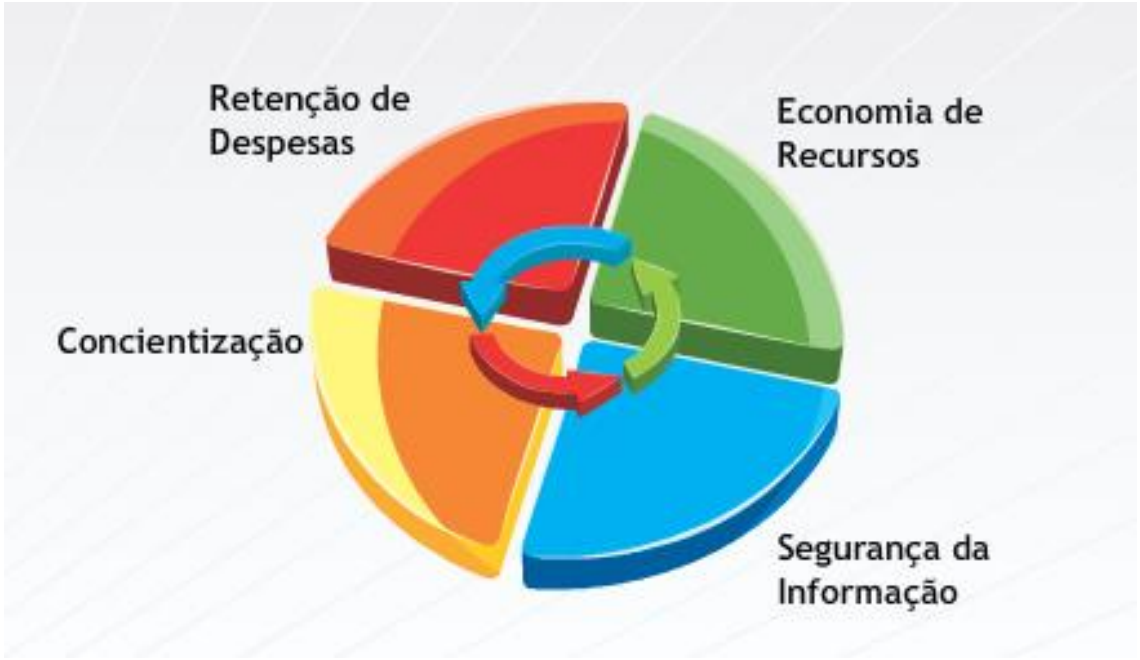
- quanto tempo essas informações/dados ficarão disponíveis,
- quando efetivamente serão descartados
- permite classificar a informação quanto a sua finalidade.

Ciclo de vida da Informação



Fonte: webaula Estácio - adaptado

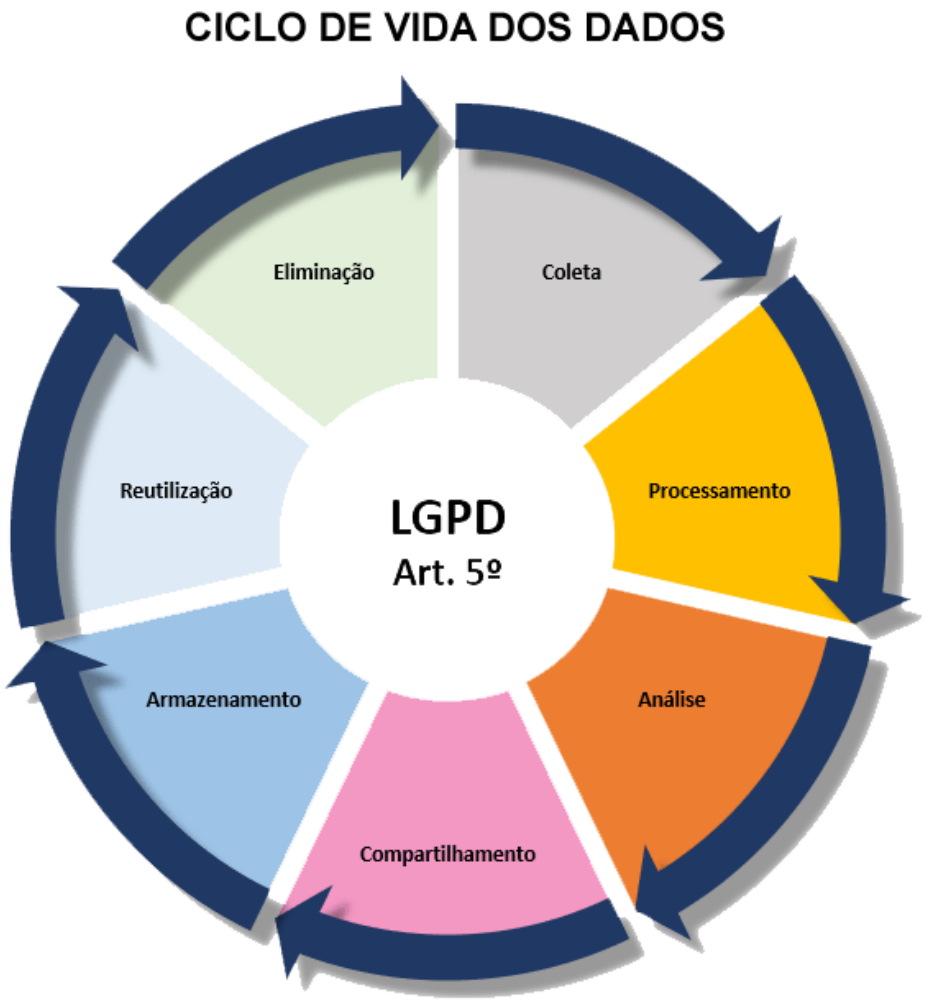
Ciclo de vida da Informação (benefícios)



- a aplicação do gerenciamento do ciclo de vida da informação traz uma série de benefícios à empresa

Fonte: webaula Estácio

Ciclo de vida dos Dados - LGPD



https://www.xpositum.com.br/ciclo-de-vida-dos-dados-e-lgpd

CICLO DE VIDA DOS DADOS		
FASE DO CICLO	**ANTES DA LGPD**	**COM A LGPD**
Coleta	Os dados pessoais são coletados indiscriminadamente.	Os dados pessoais coletados devem obedecer ao princípio da necessidade e da finalidade.
Processamento	Os dados podem ser processados sem um tratamento específico.	O processamento de dados só poderá ser realizado se o tratamento estiver enquadrado no Art. 7º da LGPD.
Análise	A análise de dados é feita para entender o mercado, conhecer o perfil das pessoas e definir estratégias para oferecer bens e serviços para o público-alvo.	A análise de dados deve levar em consideração a finalidade da coleta. Devem ser obedecidos os princípios de tratamento, com propósito legítimo, específico e explicito.
Compartilhamento	Os dados pessoais são compartilhados sem a necessidade do consentimento de seus titulares.	O compartilhamento de dados deve ser consentido pelos seus titulares.
Armazenamento	Os dados pessoais são armazenados e mantidos por tempo indeterminado.	Os dados pessoais devem ser armazenados e mantidos por prazos definidos, ou seja, até que finalidade seja alcançada ou deixem de ser necessários ou pertinentes ao alcance da finalidade.
Reutilização	Os dados pessoais são reutilizados sem a necessidade de consentimento de seus titulares.	Um novo consentimento deve ser solicitado sempre que houver mudança de finalidade.
Eliminação	Os dados pessoais são mantidos sem a obrigatoriedade de serem eliminados.	Os dados pessoais devem ser eliminados após o término de seu tratamento.

Classificação/categorização da Informação

Definição de níveis de proteção da informação, de acordo com a criticidade, valor e sensibilidade para a organização.

Estabelece o processo de acesso – forma e autorização.

Classificação usual (pode variar em cada Organização):

- **Pública** – podem ser de conhecimento público;
- **Uso interno** (corporativo) – manuseadas somente internamente à Organização.
- **Restrita** – informações estratégicas; grupos restritos;
- **Confidencial** – acesso para pessoas bem específicas da Organização.

https://www.xpositum.com.br/ciclo-de-vida-dos-dados-e-lgpd

Classificação/categorização da Informação

Quem define esses níveis?

- Verificação setorizada;
- Análise de grupo de trabalho e/ou área específica na Organização;
- Envolvimento e processo decisório da liderança;

- ampla divulgação;
- publicação de norma específica;
- inserir na Política de Segurança;
- revisão periódica.

O que é segurança?

...É estar livre de perigos e incertezas;
...É um estado ou condição que se aplica a tudo aquilo que tem valor para a organização que é chamado de ativo*;

- ativo é qualquer coisa que tenha valor para a organização;
- podem ser organizados e classificados de acordo com suas propriedades;
- permite a organização em grupos com características semelhantes no que diz respeito às necessidades, estratégias e ferramentas de proteção.

Tangível (aquilo que pode ser tocado): Informações impressas ou digitais , Sistemas, Móveis, pessoas etc.
Intangível: Marca de um produto, Imagem de uma empresa, Confiabilidade de um banco etc.

O que é segurança da Informação?

Segurança da Informação

Visa à proteção de ativos de uma empresa que contém informações.

Ativos de Informação

São aqueles que produzem, processam, transmitem ou armazenam informações.

- bancos de dados, documentações, materiais de treinamento, políticas de segurança, arquivos;
- aplicações, sistemas operacionais, ferramentas de desenvolvimento, utilitários;
- computadores, equipamentos de rede, mídias digitais Serviços: serviços de computação e redes.

Formas de proteção dos Ativos

- Preventivas - evita que acidentes ocorram;
- Desencorajamento - desencoraja a prática de ações;
- Monitoramento - monitora o estado e o funcionamento;
- Detecção - detecta a ocorrência de incidentes;
- Limitação - diminui danos causados;
- Reação - reage a determinados incidentes;
- Correção - repara falhas existentes;
- Recuperação - repara danos causados por incidentes.

Por que proteger as informações?

Fonte: webaula Estácio

Onde proteger as informações?

Do que proteger as informações?

Fonte: webaula Estácio

Fatores que impactam na segurança de uma organização

- Valor - importância do ativo para a organização;
- Ameaça - evento que tem potencial em si próprio para comprometer os objetivos da organização - danos diretos aos ativos ou prejuízos decorrentes de situações inesperadas ;
- Vulnerabilidade - a ausência de um mecanismo de proteção ou falhas em um mecanismo de proteção existente. São as vulnerabilidades que permitem que as ameaças se concretizem. (físicas, naturais, hardware, software, humanas...)
- Impacto - tamanho do prejuízo, medido através de propriedades mensuráveis ou abstratas, que a concretização de uma determinada ameaça causará; (escala de “irrelevante” até “desastroso”...)
- Risco - Medida que indica a probabilidade de uma determinada ameaça se concretizar, combinada com os impactos que ela trará.

Interação dos componentes de segurança

Fonte: webaula Estácio

Tríade da segurança da Informação

Confidencialidade: apenas as pessoas autorizadas devem acessar a informação

Integridade: a informação deve permanecer em seu estado original, sem modificações desautorizadas

Disponibilidade: a informação deve estar disponível quando solicitada pelos usuários autorizados

Outras propriedades da segurança da Informação

Autenticidade: correta identificação das partes do sistema, sejam elas: recursos tecnológicos, transações, usuários ou outros sistemas. Garantia de que a parte é quem ela diz ser.

Não-repúdio: impõe que nenhuma parte autorizada poderá negar a manipulação ou a transmissão uma informação na rede.

Autorização: prevê que o acesso a um serviço da rede seja controlado.

Auditoria: rastreabilidade dos diversos passos que um negócio ou processo realizou ou que uma informação foi submetida, identificando os participantes, os locais e horários de cada etapa

Legalidade: conformidade com um sistema de legislação.

Privacidade: a informação privada deve ser acessada apenas pelo seu dono.

Confiabilidade: o teor de uma informação ou sistema é verdadeiro.

Algumas questões sobre a segurança da Informação

- Podemos ter confidencialidade sem privacidade ?
- Podemos ter integridade sem confiabilidade ?
- Podemos ter não-repúdio sem autenticidade ?
- Podemos ter auditoria sem integridade ?

Não existe segurança absoluta!

A segurança é complexa, pois envolve aspectos de negócio, tecnológicos, humanos, processuais e jurídicos.

O aumento de funcionalidades deixam os sistemas mais inseguros.

A segurança reduz a produtividade.

É preciso equilibrar a relação entre custos e segurança.

- Isso nunca acontecerá conosco;
- Nunca fomos atacados, não precisamos de mais segurança Já estamos seguros com o firewall;
- Nossos fornecedores nos avisarão sobre alguma vulnerabilidade;
- Ninguém vai descobrir essa brecha no nosso sistema;
- Vamos colocar para funcionar, depois vemos a segurança;
- O problemas de segurança são somente da TI;
- Nosso parceiro é confiável. Podemos liberar todo acesso a ele;
- Segurança é um luxo para quem tem dinheiro.

OBRIGADO!