GESTÃO DE SEGURANÇA DA INFORMAÇÃO

O CICLO DE VIDA DA INFORMAÇÃO

Olá!

Nesta aula você irá conhecer a importância da segurança da informação, abordando os seguintes pontos:

1. Por que proteger a informação?

2. Quando proteger a informação?

3. O ciclo de vida da informação.

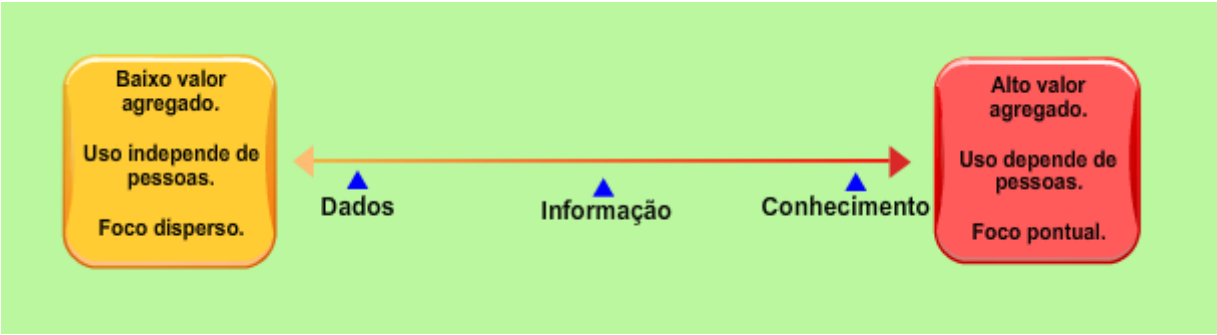
Nesta aula vamos estudar a importância da informação, por que devemos protegê-la e seu ciclo de vida.

O valor da informação para as empresas é considerado, na atualidade, como algo imensurável. Nos últimos anos, a demanda gradual por armazenamento de conhecimento tem levado à necessidade de administração desses dados de forma confiável.

Para compreendermos melhor esta questão vamos ampliar nosso o conceito de dado e 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

Percebe-se então certa hierarquia entre dado, informação e conhecimento, em que cada termo pode ser considerado como matéria-prima do termo seguinte, num crescente de agregação de valor.

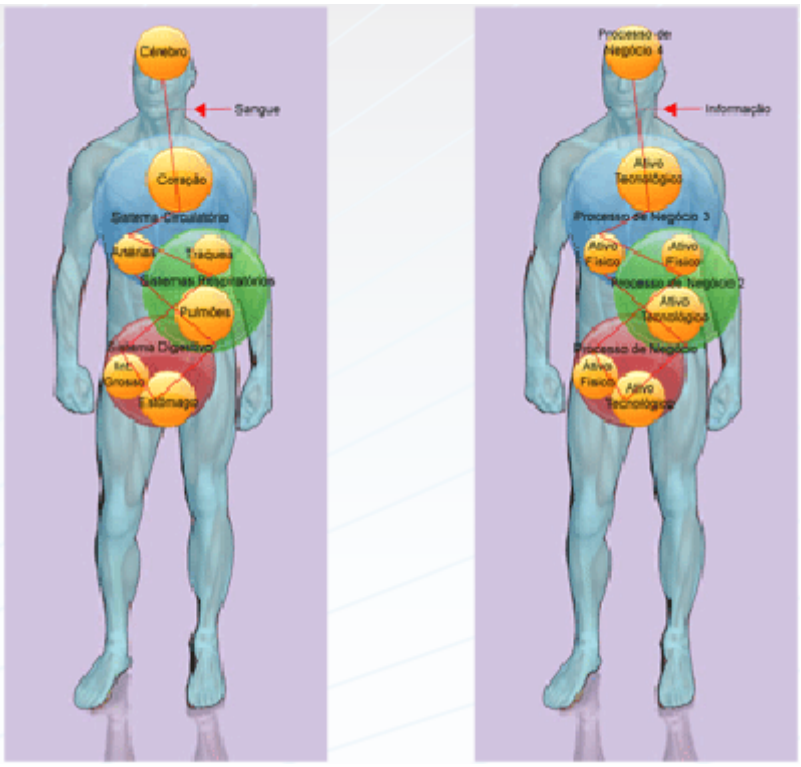


Atualmente, a informação é considerada um recurso básico e essencial para todas as organizações, sendo gerada e utilizada em todas as suas etapas de produção pelos representantes dos diversos níveis hierárquicos, além de perpassar toda a cadeia de valor, envolvendo fornecedores, clientes e parceiros.

Ciclo de vida da informação

Desde o momento em que é gerada, a informação tem um ciclo de vida dentro das corporações, passando por diversas etapas de interação até retornar ao seu ponto inicial.

Neste exemplo, segundo Sêmola, os órgãos (analogamente, ativos físicos, tecnológicos e humanos), se utilizam de sangue (analogamente, informação), para pôr em funcionamento os sistemas digestivo, respiratório, etc. (analogamente, processos de negócio), para consequentemente, manter a consciência e a vida do indivíduo (analogamente, a continuidade do negócio).



Por que proteger a informação?

Já que percebemos o quão valiosa é a informação para o negócio vamos estudar os aspectos ligados à segurança, as propriedades que devem ser preservadas e protegidas para que a informação esteja efetivamente sob controle, e principalmente, os momentos que fazem parte do seu ciclo de vida.

Como qualquer bem ou recurso organizacional, a informação também possui seu conceito de valor. Apresentamos a seguir quatro tipos possíveis de valor da informação:

Valor de uso - baseia-se na utilização final que se fará com a informação;

Valor de troca - é o quanto o usuário está disposto a pagar, conforme as leis de mercado (oferta e demanda);

Valor de propriedade - reflete o custo substitutivo de um bem;

Valor de restrição - surge no caso de informação secreta ou de interesse comercial, quando o uso fica restrito a apenas algumas pessoas;

Dado o caráter abstrato e intangível da informação, seu valor está associado a um contexto. A informação terá valor econômico para uma organização se ela gerar lucros ou se for alavancadora de vantagem competitiva, caso contrário poderá ter pouco ou nenhum valor.

Quando proteger a informação?

Armazenamento

Momento em que a informação é armazenada, seja em um banco de dados compartilhado, em uma anotação de papel posteriormente colocado em um arquivo de metal, ou ainda, em um pendrive depositado em uma gaveta, por exemplo.

Transporte

Momento em que a informação é transportada, seja ao encaminhar informações por correio eletrônico (e-mail), ao postar um documento via aparelho de fax, ou ainda, ao falar ao telefone uma informação confidencial, por exemplo.

Descarte

Momento em que a informação é descartada, seja ao depositar na lixeira da empresa um material impresso, seja ao eliminar um arquivo eletrônico em seu computador de mesa, ou ainda, ao descartar um CD-ROM usado que apresentou falha na leitura.

Manuseio

Momento em que a informação é criada e manipulada, seja ao folhear uma maço de papéis, ao digitar informaçiies recém-geradas em uma aplicação internet, ou ainda, ao utilizar sua senha de acesso para autenticação.

Agora que você já sabe PORQUE e QUANDO proteger as Informações, veremos a seguir as respostas dos seguintes questionamentos:

Onde proteger as informações?

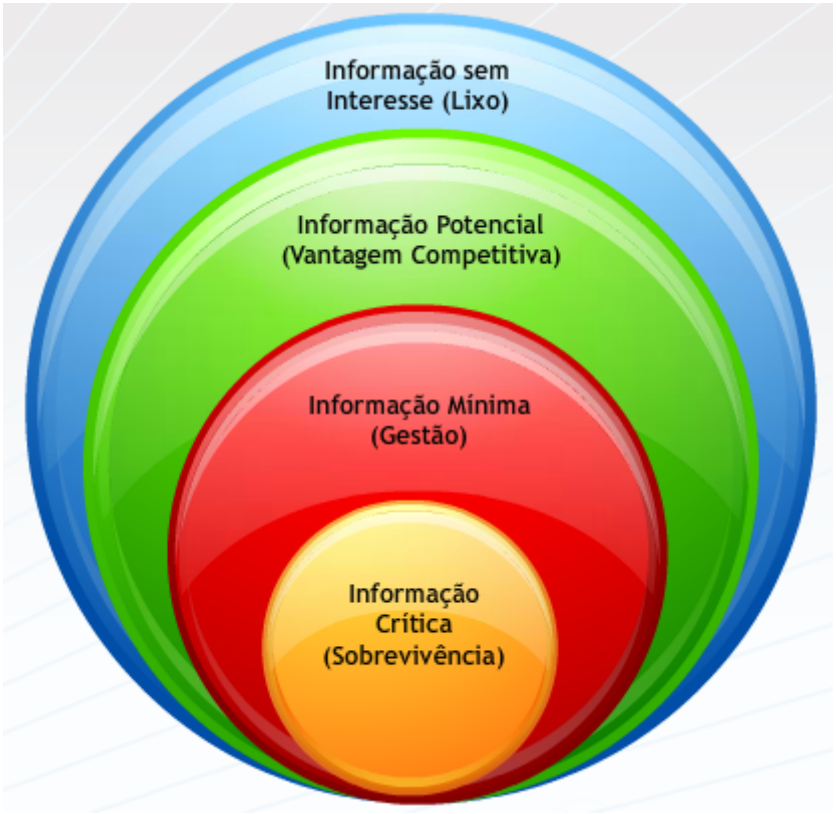
Nos ativos que as custodiam...

Do que proteger as informações?

Das ameaças...

Percebe-se então que a gestão do ciclo de vida da informação tem se tornado um elemento fundamental para a gestão dos negócios. Sendo essencial a utilização do Gerenciamento do ciclo (ILM – Information Lifecycle Management) de vida da informação, de forma a operacionalizar a informação e os dados, ou seja, organizar em meios físicos e com registros, categorizando-os para garantir a segurança e privacidade.

Este método permite que os gestores de tecnologia e os administradores da corporação definam por quanto tempo esses dados ficarão disponíveis, quando efetivamente serão descartados e permite classificar a informação quanto a sua finalidade.



Informação sem interesse (Lixo)

A informação sem interesse, ou lixo, é considerada uma parcela negativa inversamente proporcional à sua quantidade, em uma hipotética equação de valor para a finalidade da informação organizacional, e pode ser associada ao conceito de sobrecarga de informação. A relevância se manifesta através do impacto que a presença ou ausência da informação pode gerar no ambiente.

Informação Potencial (Vantagem Competitiva)

A informação potencial é dirigida principalmente para a direção da organização, apontando possíveis vantagens competitivas a serem conquistadas.

Informação Mínima (Gestão)

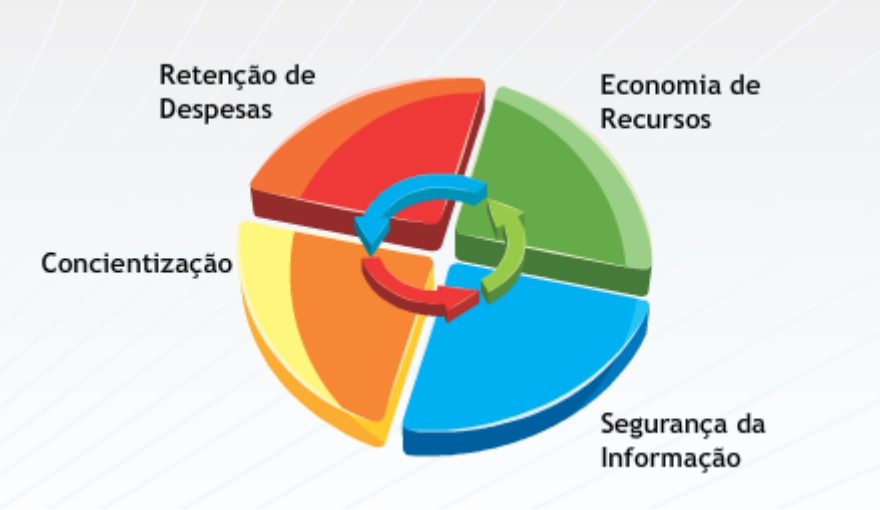
A informação mínima é destinada originalmente aos gerentes de nível intermediário para a realização de atividades de gestão organizacional.

Informação Crítica (Sobrevivência)

A informação crítica destina-se à sobrevivência da organização para atender prioritariamente às áreas operacionais.

Esta classificação permite identificar o grau de relevância e prioridade que a informação exerce em cada nível da organização.

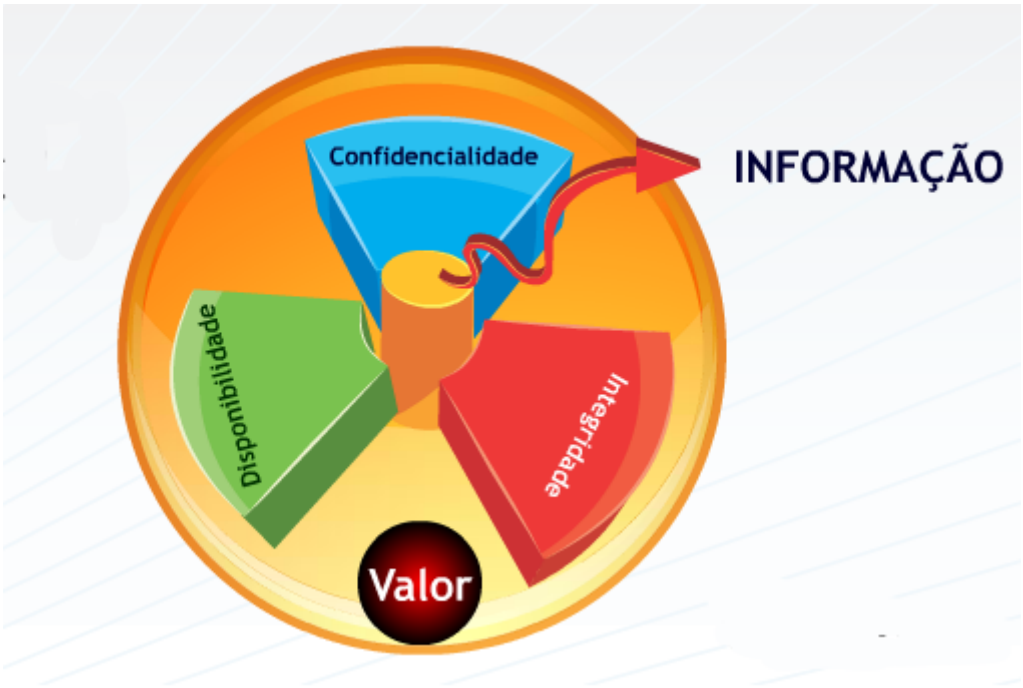
Assim a aplicação do gerenciamento do ciclo de vida da informação traz uma série de benefícios à empresa:



Classificação da Informação:

O processo de classificação da informação consiste em identificar quais são os níveis de proteção que as informações demandam e estabelecer classes e formas de identificá-las, além de determinar os controles de proteção a cada uma delas.

Existem quatro aspectos importantes para a classificação das informações. Cada tipo de informação deve ser examinado a partir desses aspectos:



Confidencialidade: A informação só é acessada pelos indivíduos autorizados.

Disponibilidade: A informação sempre está disponível quando necessária às pessoas autorizadas.

Integridade: A informação é atual, completa e mantida por pessoas autorizadas.

Valor: A informação tem um alto valor para a organização.

Saiba mais

Clique aqui e conheça outros aspectos

http://estaciodocente.webaula.com.br/cursos/gsgisi/docs/doc01_aula02_GSI.pdf

Outro fator que deve ser considerado é o nível de ameaça conhecido que cada informação tem. Para isso devem ser respondidas questões como:

Existem concorrentes buscando a informação?

É uma informação fácil de perder a integridades, ficar desatualizada?

É possível que ela dique indisponível e por qual motivo isso pode acontecer?

Com base na análise dos parâmetros anteriores, podemos chegar ao nível de segurança da informação. Um nivelamento de segurança pode seguir, por exemplo, a seguinte classificação:

Irrestrito: Esta informação é pública, podendo ser utilizada por todos sem causar danos à organização.

Interna: Esta informação é aquela que a organização não tem interesse em divulgar, cujo acesso por parte de indivíduos externos a ela deve ser evitado. Entretanto, caso esta informação seja disponibilizada ela não causa danos sérios à organização.

Confidencial (garantia de que os usuários autorizados obtém acesso à informação e aos ativos correspondentes sempre que necessário. NBR ISO/IEC 27002): Informação interna da organização cuja divulgação pode causar danos financeiros ou à imagem da organização. Essa divulgação pode gerar vantagens a eventuais concorrentes e perda de clientes.

Secreta: Informação interna, restrita a um grupo seleto dentro da organização. Sua integridade deve ser preservada a qualquer custo e o acesso bastante limitado. Esta é a informação considerada vital para a companhia.

Para podermos chegar nestes níveis de segurança podemos também considerar os seguintes aspectos:

	Confidencialidade	Integridade	Disponibilidade
Alta	Confidencial	Confidencial	Crítica
Média	Interna	Interna	Moderada
Baixa	Pública	Pública	Baixa

O que devemos notar é que o nivel de segurança pode ser aumentado tanto pela necessidade de confidencialidade quanto pela de disponibilidade. Existem os casos onde estes fatores se somam. Por exemplo, uma informação pode ter requisitos de confidencialidade média, mas a integridade alta. Assim o nivel de segurança da informação deve ser definido levando em conta todos estes fatores em conjunto e não apenas um deles isoladamente. E para isso surge a próxima questão:

Quem é que define esse nível?

Para definir o nível de segurança da informação de cada setor da organização a pessoa mais indicada é o próprio responsável daquele setor. Ele é quem certamente conhece melhor as informações do seu setor assim como as necessidades de confidencialidade, integridade e disponibilidade do setor.

Após esta classificação ser feita também é importante que alguém de um nível superior a ele esteja verificando a classificação para garantir que as informações que precisem transitar entre os diversos setores não sejam demais protegidas e isoladas em um setor e também que as informações que não podem transitar estejam protegidas.

Para finalizarmos:

O mais importante para a organização é todo o conhecimento e as informações que ela tem relativos aos processos do seu negócio específico. Aqueles que conhecem melhor da sua área tem mais ferramentas, que no caso são as informações para um melhor desempenho.

Percebe-se então que a gestão do ciclo de vida da informação tem se tornado um elemento fundamental para a gestão dos negócios. Lembrando que a informação que deve ser protegida é aquela que oferece riscos de causar danos nas operações da empresa caso seja transmitida a quem não for autorizado e que a informação que deve ser disseminada também oferece riscos de causar danos as operações da empresa caso não chegue ao seu destinatário, ou não esteja disponível na hora certa.

O que vem na próxima aula

Na próxima aula, aprenderemos o seguinte tema: Vulnerabilidade de Segurança

E, abordaremos os seguintes assuntos:

- Assunto 1: Conceitos básicos
- Assunto 2: Principais tipos de vulnerabilidades.
- Assunto 3: Ferramentas para análise de vulnerabilidade de segurança.

CONCLUSÃO

Nesta aula, você:

- Compreendeu a importância e o valor da informação, seu ciclo de vida.
- Conheceu o conceito de classificação da informação e os níveis de proteção.
- Percebeu a necessidade da gestão do ciclo de vida da informação no contexto corporativo.