SEGURANÇA E PROTEÇÃO DE DADOS

Prof. Priscilla Cunha

pcunha@uni9.pro.br

INTRODUÇÃO

- Muitas empresas pensam e adotam estratégias para a Segurança de suas Informações, porém, numa amplitude limitada.
- A Segurança vai muito além dos acessos via "usuário e senha" para esse ou aquele usuário, ou da instalação do antivírus.

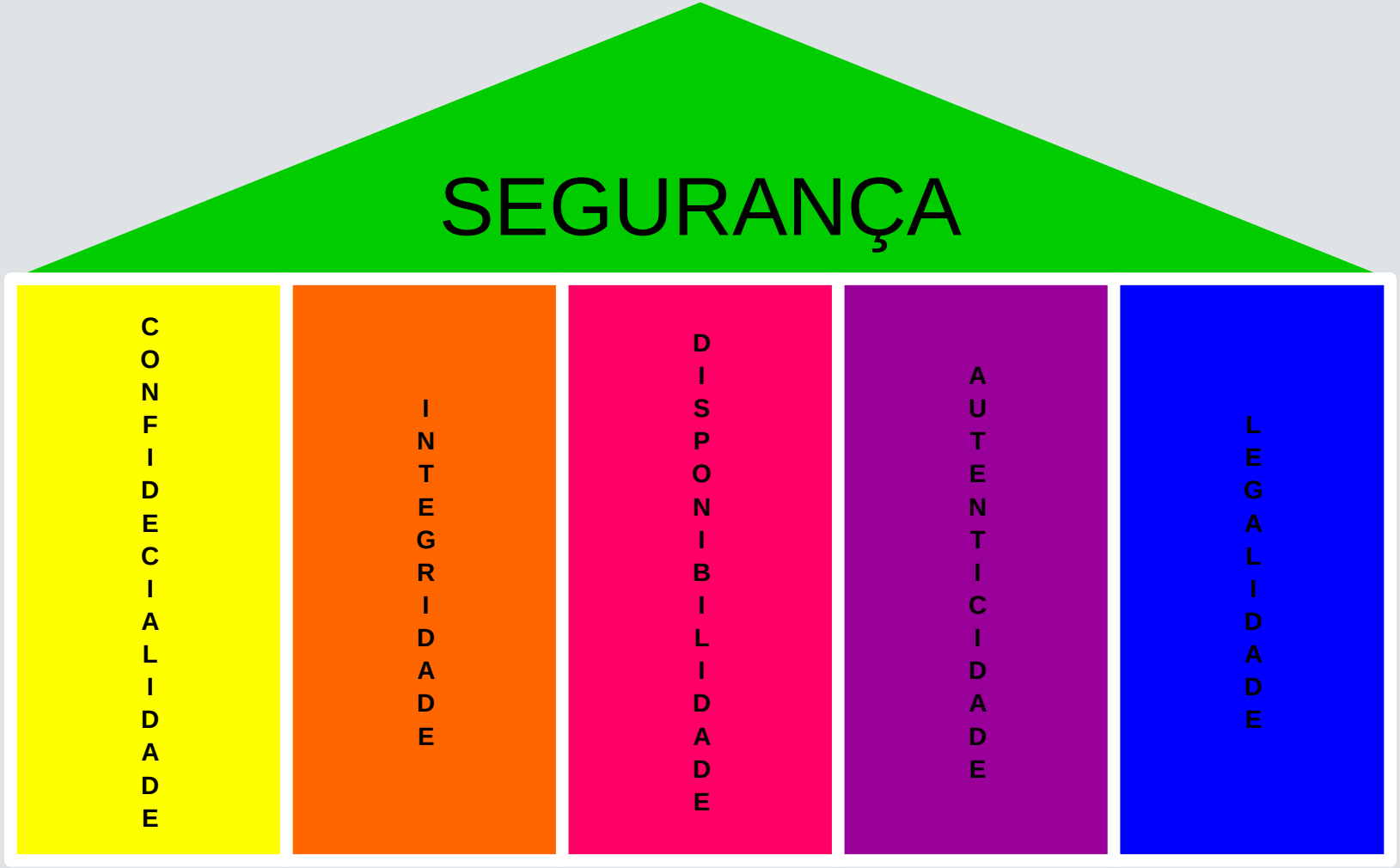
- A melhor maneira de se pensar em Segurança das Informações é seguir algumas diretrizes consagradas no mercado.
- Essas diretrizes cobrem a totalidade das providências que devem ser adotadas, a fim de que as informações das empresas passem por todo seu ciclo de vida sob a melhor maneira de estarem seguras.

- Sempre que pensamos em segurança, temos de ter em mente que precisamos garantir alguns serviços básicos.
- Esses serviços básicos são conhecidos como CIDAL e dizemos que eles são os pilares da segurança da informação.

CIDAL

CIDAL

- Confidencialidade
- Integridade
- Disponibilidade
- Autenticidade
- Legalidade


SEGURANÇA
CONFIDECIALIDADE
INTEGRIDADE
DISPONIBILIDADE
AUTENTICIDADE
LEGALIDADE

Confidencialidade

- Garantir que a informação só pode ser acessada por pessoas autorizadas.
- A definição de "quem pode" e "até onde pode" acessar carece de muita análise e discussões entre todos os envolvidos.

- Manter as informações sob a confidencialidade é adotar meios que garantam que as informações sejam acessadas somente por aqueles que tem permissão de acessá-las.
- Não existe uma fórmula ou regra a ser seguida. As empresas são diferentes e as deliberações de permissões também para cada uma.

Integridade

- Garantir que as informações não podem sofrer quaisquer alterações desde seu envio até o armazenamento, incluindo-se aqui seu transporte.
- A ideia é proteger as informações contra alterações indevidas (intencionais ou não).

- De nada servem informações não confiáveis para as empresas.
- Toda informação deve tratada como um "precioso bem" para a empresa. Assim, a empresa deve prover meios que garantam que todas suas informações sejam criadas com integridade e manipuladas sob a mesma diretriz.

- A diretriz Integridade zela para que hajam processos, previamente definidos, para toda e qualquer manipulação de informações na empresa.
- Esses processos devem seguir permissões e, se for o caso, passarem por autorizações além de prever o registro das alterações e das autorizações para eventuais auditorias.

Disponibilidade

- Garantir que as informações estarão sempre disponíveis para que as pessoas autorizadas possam acessar as mesmas quando necessitarem fazer uso delas para a execução de suas tarefas diárias.
- Hoje, as empresas estão cada vez mais informatizadas e dependentes de suas informações.

- A diretriz de Disponibilidade orienta para que a empresa defina processos a fim de que seja garantido o fornecimento de informações quando necessárias.
- Sem as informações a disposição, funcionários não trabalham, clientes ficam insatisfeitos, fornecedores não sabem sua necessidade, etc.

- Dessa maneira, a TI atualmente lida com a "alta disponibilidade", ou seja, tem que garantir que as informações possam ser acessadas quase 100% do tempo.
- Exceções são feitas aos períodos de manutenção nas bases de dados ("janelas de processamento").

Autenticidade

- Garantir que os usuários que estão acessando e usando as informações são eles mesmos.
- Devemos validar os usuários que acessam a informação garantindo que o usuário não poderá negar um acesso depois que ele o efetuar.

- Trata-se de uma diretriz de suma importância, pois orienta a empresa para que providencie processos que garantam que a pessoa ou sistema que está acessando a informação, realmente seja quem diz ser e, realmente, está autorizado a acessá-la.

- Para garantir a autenticidade, alguns métodos podem ser implementados, como:
  - Usuário e senha
  - Biometria

Legalidade

- Garantir o cumprimento das leis vigentes (federais, estaduais ou municipais) e as normas internas da empresa, zelando para que a forma como a empresa lida com as informações estejam de acordo com essas leis.

- É um grande desafio, pois pessoas habilitadas para acesso às informações nem sempre agem de maneira profissional, mas para obterem vantagens pessoais e financeiras e, aliado ao fato da ausência de mecanismos legais punitivos, gera-se com isso um ambiente vulnerável às fraudes.

- É fundamental que situações ainda não previstas em lei sejam adequadamente tratadas em códigos de ética corporativos.


Conceitos Básicos de Segurança
Não-repúdio do remetente
Irretratabilidade
Não deverá ser possível ao remetente negar o envio da mensagem.
Não negar o envio
Confidencialidade da mensagem
"Sigilo"
Só o destinatário autorizado deve ser capaz de extrair o conteúdo da mensagem da sua forma encriptada.
Só para o destinatário Autorizado
Evita acesso não autorizado
Ataque: Interceptação
Autenticação do remetente
Requer que a origem da mensagem seja corretamente identificada
O destinatário deverá ser capaz de identificar o remetente e verificar que foi mesmo ele quem enviou a mensagem.
Ataque: Criar uma mensagem falsa
Permitir que uma entidade se identifique
1 Identificação
2 Verificação
Autorização
Determina o que pode ser executado
Disponibilidade do Sistema
Sistema sempre 'no ar'
A usuário com autorização
Garantir acesso aos dados
Ataque: Interrupção da mensagem
Ex.: RAID
Integridade da mensagem
"Lacre"
Destinatário deverá ser capaz de determinar se a mensagem foi alterada durante a transmissão.
Saber se alguém viu/alterou
Evita que a mensagem seja modificada
Ataque: Modificação
www.mapasequestoes.com.br

CICLO DE VIDA DA INFORMAÇÃO

- Dentro da empresa, a informação passa por diversas etapas, e precisamos conhecer cada uma delas para protegê-la de maneira adequada.
- Cada momento deve ter seus controles e preocupações específicos.
- O ciclo de vida são as etapas pelas quais a informação passa, desde quando ela é criada até o momento em que ela não tem mais utilidade.

- O ciclo de vida é composto e identificado pelos momentos vividos pela informação que a colocam em risco. Os momentos são vivenciados quando os ativos físicos, tecnológicos e humanos fazem uso da informação, sustentando processos que, por sua vez, mantêm a operação da empresa. (Sêmola, 2003)

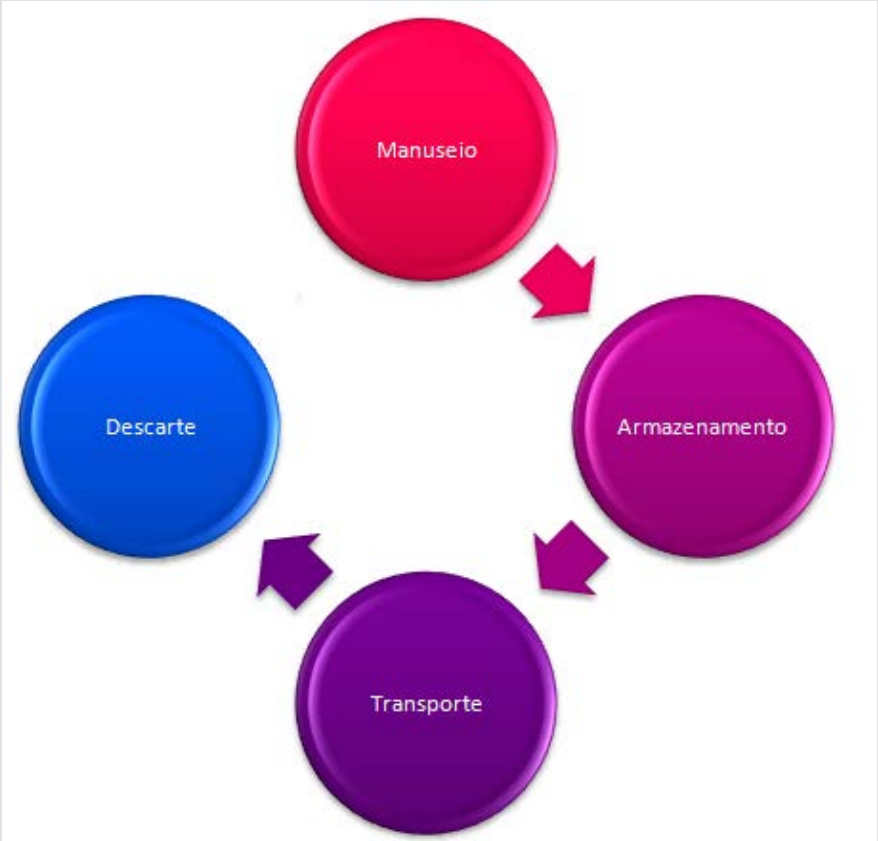
- Em geral, o ciclo de vida engloba:
  - O momento em que a informação é criada (ou manipulada) - MANUSEIO;
  - O momento em que a informação é salva - ARMAZENAMENTO;
  - O momento em que a informação é enviada - TRANSPORTE;
  - O momento em que a informação é apagada - DESCARTE.

- Manuseio: quando, como e onde a informação é criada ou manipulada. É uma etapa que pode ocorrer diversas vezes durante o ciclo de vida da informação. Ex: gráficos de despesas são gerados pelo departamento financeiro todo dia 30 usando a ferramenta MS Excel

- Armazenamento: como e onde a informação é gravada. A informação pode ser armazenada em meio físico ou lógico. Essa etapa sempre ocorre quando uma informação é criada ou alterada. Ex:o gráfico de despesas deve ser salvo no servidor XXX, na pasta YYY

- Transporte: quando a informação é transmitida, deixa seu local original. Quando a informação sai de um local e vai para outro. Ex: o gráfico de despesas só pode ser enviado pelo email corporativo

- Descarte: quando a informação é completamente eliminada. Quando o uso da informação é encerrado, quando ela não é mais necessária de maneira alguma. Ex: apagar do servidor e dos itens enviados e destruir os impressos que foram gerados.



Manuseio
Está correto?

Armazenamento
É adequado?

Transporte
É seguro?

Descarte
É permanente?

CLASSIFICAÇÃO DA INFORMAÇÃO

- O ato de classificar algo refere-se a organizar um ou mais itens de acordo com suas características comuns, colocando-os em ordem.
- Podemos classificar quase tudo, desde roupas em um armário, produtos em um supermercado, livros, DVDs, brinquedos, informações, etc..

- Classificar envolve escolher a melhor alternativa de se colocar algo em ordem.
- O primeiro passo da classificação é a determinação de um parâmetro de classificação e a definição dos rótulos de classificação.
- Devemos ter em mente que TODA a informação deve ser classificada.

- Por exemplo: podemos classificar filmes pelo parâmetro gênero, usando os seguintes rótulos: terror, suspense, ação, policial, comédia, ficção, romance e desenho animado.

- Precisamos classificar as informações pois as empresas possuem diversos tipos de informação, todas elas com necessidades de segurança diferentes. Mas esse é um processo complexo, devido ao volume de informação que as empresas possuem.

- Existem informações em uma empresa que necessitam de um alto nível de proteção, enquanto outras não.
- Quanto mais informatizado um ambiente for, e com mais pessoas acessando as informações, mais vulnerabilidades teremos.

- Classificando a informação podemos:
  - Identificar situações de risco
  - Adotar procedimentos de segurança adequados a cada tipo de informação

- Fazendo a classificação da informação adequada pode-se definir os procedimentos e tecnologias para garantir o CID; com a classificação da informação realizada, pode-se definir melhores regras de controle de acesso.

- Para se classificar a informação, é preciso criar um roteiro de como esse processo será feito, tendo o aval da alta administração e definindo, previamente, quais rótulos serão utilizados.

- A classificação da informação vai permitir identificar uma situação de risco mais facilmente e reagir em menor espaço de tempo.
- Além disso, a classificação da informação gera redução de custos e aumento da segurança.

- Classificando as informações de acordo com sua sensibilidade e controlando o acesso de acordo com essa classificação, a empresa poderá definir os modelos e as tecnologias que utilizará para preservar o CID.

- A classificação da informação deve ser abrangente para que seja eficiente, considerando todos os tipos de informação da empresa e todas as etapas de seu ciclo de vida.

- Os rótulos mais comumente usados na classificação da informação são:
  - Secreta
  - Confidencial
  - Restrita
  - Interna
  - Pública

- Secreta: informação que é um diferencial competitivo, referente às estratégias de negócio. Trata-se da informação cuja perda ou acesso indevido pode ocasionar em grandes perdas financeiras e, por vezes, em encerramento das atividades da empresa. Ex: fórmula da coca-cola;

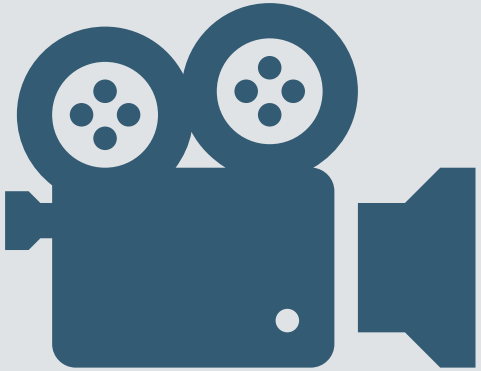
- Confidencial: informação restrita ao alto escalão da empresa e àqueles que eles determinarem (para a execução de suas tarefas). Em geral são informações estratégicas e administrativas. Ex: projeto para compra de um concorrente;

- Restrita: informação de acesso apenas para os usuários que precisam fazer uso da mesma em suas tarefas. Ex: apenas o RH e o financeiro acessam a folha de pagamento;

- Interna: informação cujo uso é possível apenas dentro da empresa e deve ser liberado a todos que nela atuam. Geralmente trata-se de informações técnicas ou organizacionais. Ex: calendário de eventos e treinamentos;

- Pública: informações que podem estar disponíveis para qualquer um. Ex: relação de produtos a venda pela empresa.

VÍDEOS



- CIDAL - https://www.youtube.com/watch?v=cQe05kUbAtQ
- https://www.youtube.com/watch?v=tc1vnk7t9kw

PARA SABER MAIS

- Um dia, o hacker bate à porta
- https://oglobo.globo.com/sociedade/tecnologia/um-dia-hacker-bate-porta-2788750

- https://www.teleco.com.br/tutoriais/tutorialitil/pagina_2.asp

- https://senhasegura.com/pt-br/os-pilares-da-seguranca-da-informacao/


Dúvidas?
Não mais..