Classificação da informação – exemplo de possíveis classificações nas empresas

Descrever o ciclo de vida da informação, fator importante para que se possa identificar e localizar as informações dentro dos processos internos da empresa, bem como apresentar os principais aspectos relacionados à necessidade da classificação e à informação dentro das organizações como forma de facilitar o processo da análise de risco.

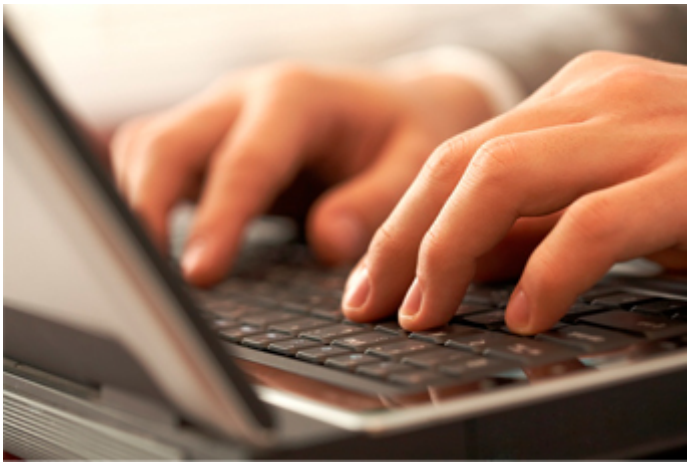
O ciclo de vida da informação

Para que se possa proteger a informação dentro da empresa é necessário conhecer o seu ciclo de vida de forma a colocar os controles específicos em cada um dos seus momentos.

O ciclo de vida, por sua vez, é composto e identificado pelos momentos vividos pela informação que a colocam em risco. Os momentos são vivenciados justamente quando os ativos físicos, tecnológicos e humanos fazem uso da informação, sustentando processos que, por sua vez, mantêm a operação da empresa. (Sêmola, 2003, pg.9)

O ciclo de vida caracteriza as várias etapas de uma informação, desde sua criação até o momento em que ela não tenha mais utilidade. É composto e identificado pelos momentos em que ativos físicos, tecnológicos e/ou humanos usam a informação. Geralmente o ciclo de vida de uma informação é representado pelos momentos em que ocorre a manipulação inicial, depois ocorre o seu armazenamento, depois a informação pode ser enviada e, por fim, pode ter o término da sua utilização.

O primeiro momento é quando a informação é criada ou manipulada. Esse momento pode ser durante uma digitação de um texto, carta, relatório, e-mail, na digitação de uma senha etc. e pode ocorrer várias vezes durante o ciclo de vida da informação.



O momento relacionado ao armazenamento é a ocasião em que a informação é guardada, ou seja, armazenada em algum meio físico ou lógico como, por exemplo, quando ela é anotada em um pedaço de papel, ou é guardada em arquivos físicos ou eletrônicos ou quando é guardada em um banco de dados ou em uma mídia (CD, DVD, HD, disquete, etc.). Ocorre sempre que há uma inclusão ou alteração da informação.

O momento relacionado ao envio da informação ocorre quando ela sai de um determinado local e vai para outro, podendo ser, por exemplo, transmitida de um local para outro através de uma rede local de computadores, ou quando a que circula por meio de um aparelho de FAX ou até mesmo um relatório em papel que é transportado por um funcionário entre um departamento e outro da empresa.

O momento do término da sua utilização é o momento em que a informação é eliminada, apagada, destruída de forma definitiva. Por exemplo: ao jogar no lixo um relatório; ao apagar um arquivo do computador; ao jogar fora um CD/DVD ou mesmo um computador que não tem mais utilidade.

Termos importantes

Quando estamos pensando no assunto segurança da informação, existem algumas palavras que ajudam a justificar a necessidade da implementação dos controles de segurança frente à alta administração da empresa.

Dentro do assunto segurança da informação, a palavra disponibilidade está relacionada ao fato das informações e dados estarem sempre disponíveis para as pessoas que necessitam dela para executar suas tarefas diárias e cotidianas.

A palavra integridade está relacionada ao fato dos dados e das informações não terem sofrido nenhuma alteração do seu formato inicial desde o envio até o recebimento dessa informação. A ideia é que os dados e as informações estejam protegidos contra alterações indevidas, intencionais ou acidentais.

Quando nos referimos à palavra confidencialidade, estamos nos referindo somente às pessoas autorizadas que podem ter acesso aos dados ou à informação acessada. Envolve a privacidade e a proteção da informação pessoal ou corporativa.

A palavra autenticidade está relacionada à validação de uma forma que não deixe dúvidas sobre um dado ou informação, ou seja, não pode permitir o "não repúdio", que é a ação de alguém em informar que não é o responsável pelo acesso à informação ou dado. Dessa forma, as informações devem estar protegidas por controles que permitam identificar o seu autor definitivamente, sem que seja possível haver uma negação de autoria por parte dele.

A palavra legalidade está relacionada ao fato de que tudo deve estar de acordo com as leis ou legislações existentes.

A palavra "Humano" está relacionada aos fatores como consciência, individualidade e necessidades básicas que os usuários da organização possuem e que geralmente entram em conflito com as medidas de segurança.

Os usuários autorizados, que geraram ou adquiriram a informação, devem ter acesso a ela sempre que for necessário para o desenvolvimento de suas tarefas. Nesse cenário são verificados se os controles definidos atendem às especificações das leis de forma a poder identificar, controlar e, se for o caso, punir os responsáveis.

Por último, citamos a palavra **administraçâo**, que ajuda o profissional responsável pelos processos de segurança a se organizar e a acompanhar as constantes mudanças no cenário da segurança da informação.

Introdução - conceito de classificação

Quando vamos ao supermercado fazer nossas compras semanais, quinzenais, mensais ou até mesmo uma compra isolada, ficamos tranquilos, pois certamente encontraremos o produto que estamos necessitando ou algo **"parecido"**.

A palavra anterior entre aspas e em negrito é para ressaltar que teremos uma grande facilidade para encontrar produtos semelhantes no supermercado e eles sempre estarão localizados próximos um do outro. Por que isso ocorre? A resposta é simples, antes dos produtos serem colocados nas prateleiras, eles foram separados por grupos e organizados por características que possuíam e que permitiam que fossem categorizados.

Sem essas características específicas, ficaria muito difícil para separá-los e colocá-los lado a lado.

O processo de classificação significa uma ação ou efeito de colocar algo em uma determinada ordem.

Esse conceito pode ser aplicado para qualquer coisa como, por exemplo, materiais, equipamentos, objetos, ideias e também a informação. Dessa forma, tudo que possui uma característica comum e que permite que haja um processo de diferenciação entre outros elementos pode ser classificado.

Quando estamos classificando, estamos escolhendo, dentre as alternativas possíveis para isso, a melhor forma de colocar em ordem algo.

Para que possamos fazer uma classificação eficiente, faz-se necessário que sempre consigamos criar parâmetros que serão utilizados como ponto de apoio nas nossas decisões.

O parâmetro, ou seja, "definição" do que é determinado item, é o que nos ajudará no processo de classificação, pois pessoas diferentes têm ideias e conceitos diferentes, e para que haja um consenso, as definições dos rótulos usados para classificar a informação devem estar muito bem definidas.

No nosso caso, o principal problema que temos está em classificar os tipos de informações existentes dentro das empresas de forma que possamos colocar o nível de segurança da informação adequado para cada situação. Afirmamos isso porque uma informação que pode ser acessada por todas as pessoas, tanto funcionários e colaboradores da empresa como pessoas que não pertencem a ela, deve ter um nível de proteção diferente de outra que deve ser acessada apenas pela alta administração da empresa, ou seja, pelos seus diretores.

Fica claro que no cenário anterior existirão dentro da empresa informações que não precisam

de proteção, ao contrário de outras que deverão ser protegidas de forma excessiva, consumindo recursos materiais e humanos para sua administração e manutenção.

A principal razão para classificar as informações é que elas não possuem os mesmos níveis de confidencialidade, ou ainda, as pessoas podem ter interpretações diferentes sobre o seu grau. Quanto mais informatizado estiver o ambiente de informação, maior será a vulnerabilidade em razão da quantidade exponencial de acesso de seus usuários. Além disso, a resposta a determinados tipos de situações varia de pessoa para pessoa, e de acordo com as condições do momento, especialmente se não houver um critério de julgamento claro para se avaliar o que é certo ou errado.

Podemos dizer que o processo de classificação da informação é um dos processos mais difíceis de serem feitos dentro de uma empresa, uma vez que a grande maioria delas não possui seus processos internos mapeados e isso acaba por dificultar na ora de se encontrar a informação e verificar a sua real importância para uma determinada atividade.

Como fazer um processo completo de classificação, ou seja, classificar todas as informações é muito difícil, devemos dar primeiro atenção às informações prioritárias para execução das principais atividades da empresa e depois continuar o processo com as demais.

Política de classificação

Para que possamos colocar em prática o processo de classificação da informação dentro da empresa, faz-se necessário existir algo que possa dar apoio ao processo e quando falamos em apoio, estamos nos referindo à criação de documentos definidos pela alta administração da empresa

A esses documentos damos o nome de política de classificação da informação, que permitirá que todas as ações planejadas para o projeto de classificação da informação possa ser implementado. Por meio dela poderemos definir, ou seja, rotular os tipos de classificações aprovadas pela empresa, bem como os seus respectivos critérios de avaliação e necessidade de proteção.

Uma política representa um conjunto de leis, normas e procedimentos que ajudam a colocar uma ordem em um determinado processo. A política de classificação da informação deve, sem dúvida, ser considerada o início do processo de implementação de uma estratégia de segurança em uma empresa, pois ela nos fornecerá critérios para identificarmos quais informações têm valor para a empresa e, como as pessoas devem proceder ao manipulá-las.

Com a classificação da informação, pode-se identificar uma situação de risco mais facilmente e reagir em menor espaço de tempo, além de que, ao adotar procedimentos e ferramentas de proteção adequadas a cada tipo de informação, ocorre uma 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 organização poderá definir os modelos e as tecnologias que utilizará para preservar a confidencialidade, integridade e disponibilidade dos seus dados.

O processo de classificação tenta obrigar que todos os funcionários e colaboradores da empresa passem a pensar e incorporar ideia da classificação no seu dia a dia, protegendo assim, as informações que estarão sob a sua guarda ou responsabilidade.

Toda informação classificada, quando passar por alteração de conteúdo, deve ser submetida a novo processo de classificação, com o objetivo de rever o nível mais adequado (FERREIRA, 51).

A norma de classificação da informação

A norma de classificação da informação deve ser abrangente para ser eficaz, considerando todos os tipos de informações e também todas as etapas de seu ciclo de vida, como vimos anteriormente ao falar sobre o esse assunto.

As informações poderão receber diversos rótulos de classificação e tudo dependerá do que for acordado entre os responsáveis. Abaixo seguem alguns rótulos comumente utilizados dentro das empresas

Rótulo da Informação	**Detalhe ***
Secreta	Trata-se da informação cuja perda ou acesso indevido possa significar paralização nos processos da empresa, bem como perdas financeiras e abalo da imagem.
Confidencial	Trata-se da informação que deve ser acessada apenas pela alta administração da empresa ou por quem ela determinar para a execução de suas tarefas, não podendo ser divulgada total ou parcialmente, em qualquer formato a outros usuários não designados.
Restrita	Trata-se da informação cujo acesso deve estar liberado apenas aos usuários/colaboradores que dela necessitam para cumprir suas tarefas.
Interna	Trata-se da informação cujo acesso e uso deve ser liberado apenas aos funcionários/colaboradores da empresa e cujo conteúdo seja de assuntos técnicos ou organizacionais que tornam seu uso possível somente dentro da empresa.
Pública	Trata-se das informações que podem ter o seu acesso liberado para qualquer pessoa dentro ou fora da empresa, sem que exista qualquer restrição na sua exibição/uso e cuja divulgação indevida não acarrete impacto à empresa.

*Apenas um exemplo de explicação para o rótulo da informação de forma que todos tenham o mesmo entendimento.

Algumas empresas possuem em sua política de classificação da informação o costume de, além de classificar a informação por rótulos, atribuir cores ou figuras que ajudarão na identificação de algum item classificado de forma mais imediata. Como por exemplo, as informações secretas poderiam ser classificadas com um círculo vermelho que sempre deveria ser colocado no canto superior direito de qualquer documento impresso.

Clique no botão a seguir e teste sua memória e aprendizado entretendo-se com a cruzadinha.

objeto disponível apenas na versão web

Agora que você já estudou esta aula, resolva os exercícios e verifique seu conhecimento.
Caso fique alguma dúvida, leve a questão ao Fórum e divida com seus colegas e professor.

objeto disponível apenas na versão web

A seguir, preencha a(s) lacuna(s) com a(s) palavra(s) adequada(s) às afirmações.

Referências

FERREIRA, Fernando Nicolau Freitas; ARAÚJO, Márcio Tadeu de. *Política de Segurança da Informação*: guia prático para elaboração implementação. Rio de Janeiro: Ciência Moderna, 2006.

MAGALHÃES, Ivan Luizio; PINHEIRO, Walfrido Brito. *Gerenciamento de Serviços de TI na Prática*: uma abordagem com base na ITIL. São Paulo: Novatec, 2007.

SÊMOLA, Marcos. *Gestão da Segurança da Informação*: uma visão executiva. Rio de Janeiro: Elsevier, 2003.