Classificação da Informação

Bruno Reis, Jimmy Costa Mota, Patryck Pabllo Borges de Oliveira.

Universidade Católica de Brasília (UCB), Campos Universitário II, SGAN 916 – Módulo B – Brasília – DF – Brasil.

{bruno_p_reis@hotmail.com, heydjo@yahoo.com.br, patryckpabllo}

Abstract. *Information classification is of utmost value to the organizations because it allows the organization to direct its resources for information security. By knowing the integrity, availability and confidentiality levels of each piece of information the organization is able to create optimized and specific security policies. This article shows a way to classify the information into an organization, by identifying specific criteria and relevant practices. It also defines suggestions of practices that can be taken to implement information security to each suggested level of classification.*

Resumo. *A classificação da informação é fundamental para que as organizações possam direcionar os seus recursos para sistemas de segurança. Sabendo o nível de disponibilidade, confidencialidade e integridade das informações com quais a organização trabalha, esta pode gerar políticas de segurança da informação otimizadas e específicas para cada recurso. Este texto mostra uma forma de se classificar a informação de uma empresa, se identificando os critérios e práticas relevantes. Ele também define idéias de práticas que podem ser tomadas para implementar a segurança da informação aos diversos níveis de classificação sugeridos.*

1. Introdução

Diversos procedimentos são adotados constantemente pelas organizações para garantir a segurança das informações. Salas-cofre, sistemas de criptografia, políticas e treinamento de funcionários e muitos outros procedimentos são adotados constantemente pelas organizações que para isso investem grandes quantias de dinheiro. Entretanto nem sempre esse dinheiro é bem investido pois muita informação desnecessária pode ser guardada por estes procedimento. Um exemplo pode ser um servidor de e-mail com e-mails pessoais, mantido dentro de uma política de backup e segurança rígida.

O fato é que para implementar uma boa política de segurança é necessário se conhecer a importância das diversas informações recebidas,utilizadas, armazenadas e transmitidas pela organização. É a isto que este trabalho se propõe, uma metodologia para classificação das informações de uma organização. Isto visa facilitar o trabalho de segurança, permitindo se definir o nível de segurança que deve ser utilizado no armazenamento e transmissão das informações por esta metodologia categorizadas.

Este trabalho faz com que a organização economize e direcione melhor os seus recursos com segurança da informação. Esta classificação da informação serve também para a organização conhecer melhor a o escopo, as rotas e necessidades de informação com que trabalha podendo fazer com que a informação tenha o fluxo necessário para o bom desenvolvimento dos seus trabalhos. Ou seja, este trabalho facilita também que a informação esteja mais disponível na hora certa e para a pessoa certa.

2. A Importância da Informação

A informação se situa entre o que podemos chamar de dado puro e o conhecimento. Ela consiste em um dado com uma interpretação sobre ele e, assim como o conhecimento, é muito importante nesta era atual, que vem sendo denominada de era da informação. Vejamos dois paradigmas desta era que a primeira vista podem até parecer paradoxal:

- Na sociedade da informação, a informação é o principal patrimônio da empresa e está sob constante risco, precisando assim ser seguramente armazenada e protegida.

- Na sociedade da informação, a informação é o principal ativo da empresa e precisa ser constantemente disseminada e trabalhada.

Estas idéias têm em comum o reconhecimento que o uso efetivo da informação permite que uma organização aumente a eficiência de suas operações e representa um diferencial competitivo em relação aos concorrentes. Nesta era costuma se dizer que uma organização é as duas ou três coisa que ela faz de melhor. Isto quer dizer que 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 se desempenharem melhor.

Assim sendo ambos os paradigmas citados acima são verdadeiros e devem ser considerados para o bom desempenho da empresa. A informação que deve ser protegida com riscos de causar danos nas operações da empresa caso seja transmitida a quem não for autorizado e há a informação que deve ser disseminada, também com riscos de causar danos as operações da empresa caso não chegue ao seu destinatário, ou não esteja disponível na hora certa.

3. Classificando a Informação

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

Integridade – a informação é atual, completa e mantida por pessoas autorizadas.

Disponibilidade - a informação está sempre disponível quando necessária ao pessoal autorizado.

Confidencialidade – a informação só é acessada pelos indivíduos autorizados.

Valor – a informação tem um alto valor para a organização.

Outro fator que deve ser considerado ao se gerar uma política de segurança é o nível de ameaça conhecido que cada informação tem. Para isso devem ser respondidas questões como: Existem concorrentes buscando a informação? É possível que ela fique indisponível e por qual motivo isso pode acontecer? É uma informação fácil de perder a integridade, ficar desatualizada?

4. Níveis de Segurança

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

Irrestrito – Esta informação é pública, podendo se 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 – 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 e seguro. Esta é a informação considerada vital para a companhia.

Para podermos chegar nestes níveis de segurança pode nos guiar também pela seguinte tabela apresentada por [Peltier]

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

O que devemos notar é que o nível de segurança pode ser aumentado tanto pela necessidade de confidencialidade quanto pela de disponibilidade. Uma informação que deve estar sempre disponível deve ter um serviço robusto trabalhando para isso, assim como uma informação confidencial também. E existem ainda os casos onde estes fatores se somam. Por exemplo, uma informação pode ter requisitos de confidencialidade média, mas integridade alta. Assim o nível 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 que é quem define este nível.

5 Estabelecendo Responsabilidades

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.

Além do responsável pela classificação é preciso também estabelecer os responsáveis pela manutenção dos níveis de segurança definidos. Neste caso todos os funcionários devem ser envolvidos e deve ser criado um plano com um regime de responsabilidades claro e disponível para todos. Além disso, deve ser feito um treinamento para passar os dados deste plano e se possível deve haver um supervisor que verifique a efetivação do plano nos diversos setores da organização.

6 Implementando a Classificação

Para a implementação da categorização devem ser consideradas as seguintes práticas:

- Identificação/Marcação dos Recursos Informacionais;
- Armazenamento da Informação;
- Transmissão de Informações;
- Eliminação de Informação Desnecessária
- Garantia da Integridade da Informação
- Permissão de Acesso Apropriado
- Estabelecimento de Responsabilidades

Vejamos alguns exemplos destas implementações:

6.1 Para a Identificação/Marcação dos Recursos Informacionais

Tipo do Documento	Procedimento
Documento em Papel	Caso seja gerado dentro da organização deve apresentar o nível de segurança no rodapé de todas as páginas e na capa. Caso venha de fora deve ser marcado com uma etiqueta ou carimbo.
E-mail	Deve ter o nível de segurança identificado no título.
Documentos Eletrônicos.	Deve conter o nível de segurança na "meta data" do documento. Deve conter o departamento que criou o documento e a data. Caso seja um documento que venha a ser impresso deve apresentar o nível de segurança no rodapé de todas as páginas e na capa.

Dados, bancos de dados e aplicações.	Deve conter o nível de segurança na "meta data" do documento. Os relatórios gerados devem seguir os padrões para documentos eletrônicos.
Outros tipos de mídia.	A classificação de segurança deve ser visível por etiquetas ou outros recursos que se façam necessários

6.2 Para o armazenamento das informações, de acordo com sua classificação.

Classificação	Impressos	Documentos Eletrônicos
Irrestrito	Sem requisitos especiais	backups regulares para garantir a integridade e disponibilidade.
Protegido	Guardado em local seguro (sala trancada)	Armazenado em áreas restritas do sistema operacional.
Confidencial	Guardado em local seguro com acesso restrito. Deve ter uma política de "mesa limpa"	Armazenado em áreas restritas do sistema operacional com verificação de senha.
Secreta	Guardado em zona segura com controle de acesso. Política de mesa limpa.	Armazenado em áreas restritas do sistema operacional com verificação de senha. Encriptado e com trilhas de auditoria.

	Trilha de acesso para todos os pontos de acesso (assinatura).	

6.3 Para transmissão das informações

Classificação	Impressos	Documentos Eletrônicos
Irrestrito	Sem requisitos especiais	Sem requisitos especiais
Protegido	Envelope lacrado Carta registrada.	Criptografia ou senhas em arquivos transmitidos
Confidencial	Envelope lacrado marcado com carimbo "confidencial" Notificação de Recebimento.	Criptografia ou senhas em arquivos transmitidos utilizando uma rota segura. Confirmação de recebimento
Secreta	Envelope com duplo lacre transportado sob custódia.	Criptografia ou senhas em arquivos transmitidos utilizando uma rota segura. Confirmação de recebimento Auditoria completa do processo

6.4 O descarte de informações

O lixo de certas empresas pode vir a ser uma grande fonte de informações confidenciais caso as mesmas não se preocupem com o descarte das informações. De nada adianta um relatório ser confidencial, acessado com uma boa senha e transmitido com criptografia caso ele seja impresso e o papel jogado no lixo sem as informações serem eliminadas. Assim toda mídia impressa que contenha informações relevantes deve ser destruída antes de ser descartada. Isso pode ser feito por picotadores de papel.

6.5 Protegendo a integridade

Para a proteção da integridade nos documentos eles devem todos conter informações que identifiquem sua origem assim como um carimbo caso se faça necessário. No caso de documentos eletrônicos eles devem ser controlados através de esquemas de permissão de acesso, restringindo a possibilidade de gravação aos usuários autorizados.

Caso a necessidade de integridade seja alta, certos documentos devem ser armazenados em uma localização central, só podendo ser retirados sob-custódia e com tempo limitado.

6.6 O acesso as informações

O acesso às informações deve ser feito de acordo com as políticas estabelecidas para o armazenamento das mesmas.

6.7 Responsabilidades

Após as responsabilidades serem estabelecidas e definidas e os treinamentos serem feito cada funcionário deve assinar um termo de responsabilidade indicando sua concordância com a política estabelecida.

7 Um Processo para a Implementação da Classificação

Para implantar a classificação proposta, considerando as práticas acima, podemos seguir os seguintes passos:

- Inventário
- Classificação de Risco
- Definir Política da Organização
- Definir Políticas por Projetos
- Implementação de Práticas de Segurança
- Treinamento
- Identificação (marcação)
- Monitoramento

8 Conclusões

Com uma boa classificação das informações a organização não só poderá ter uma boa e otimizada política de segurança da informação como também terá outros benefícios. Ela poderá conhecer melhor os seus processos, pois se verá forçada a fazer um inventário das informações, poderá também conhecer as informações que precisa disponibilizar para seus clientes e que ainda não têm um canal apropriado para isso.

Porém o trabalho de classificação da informação é um trabalho maior do que pode parecer a primeira vista pois envolve todos os departamentos de uma organização assim como seus responsáveis, além disso pode mexer ou expor algumas estruturas de poder dentro da organização.

Assim sendo este trabalho deve **ser** feito por uma equipe competente **e** diversificada onde haja um patrocinador da alta gerência com motivação suficiente para poder tocar o projeto pois caso contrário o mesmo está sujeito a não ter o sucesso esperado.

9 Referências

[PELTIER] PELTIER, Tomas R., “Standardinzing Information Classification”, Disponível em: http://searchsecurity.techtarget.com/tip/1,289483,sid14_gci995767,00.html?Offer=SEcpcc42005

[DAVENPORT] DAVENPORT, T.H., “Ecologia da Informação: porque só a tecnologia não basta para o sucesso da era da informação”, Trad. Bernadete Siqueira. São Paulo, 1998.

[ABREU] ABREU, Dimitri., “Melhores Práticas para Classificar as Informações”. Módulo e-Security Magazine. São Paulo, agosto 2001. Disponível em: http://www.modulo.com.br

[SECURENET] SECURENET, “Gerindo Práticas de Segurança da Informação”, Abril 2001, Disponível em http://www.securenet.com.br/artigo.php?artigo=94