

1.Responsabilidade pelos ativos

Os ativos de negócio são necessários para uma organização. Eles custam dinheiro ou possuem certo valor.

Os ativos de negócio incluem:

- Informações na forma de documentos, base de dados, contratos, documentação de sistemas, procedimentos, manuais, logs de sistemas, planos e guias
- Programas de computador, tais como programas do sistema, programas do usuário e programas de desenvolvimento.
- Equipamentos como servidores, PCs, componentes de rede e cabos
- Mídias como CD_ROMs, pen drives, HDs externos e outros
- Serviços como construções, equipamentos de fabricação, instalações de distribuição e outros
- Pessoas e seus conhecimentos
- Ativos não tangíveis, tais como a imagem e a reputação da organização

Os ativos da empresa devem ser classificados a fim de permitir a definição de níveis de segurança para eles. Isso é responsabilidade do proprietário. Cada ativo deve ter um dono e deve ser registrado em uma base de dados gerenciada de forma centralizada

Um bom e completo registro dos ativos da empresa é necessário para a análise de riscos. Adicionalmente, às vezes os registros são necessários para seguros, contabilidade financeira e requisitos legais.

As informações que são gravadas sobre um ativo da empresa são:

- O tipo de ativo da empresa
- O dono
- A localização
- O formato
- A classificação
- O valor para o negócio
- O custo inicial
- A idade
- O custo estimado de reposição

Essas informações podem ser necessárias para a recuperação que se segue a um incidente ou desastre. O dono é a pessoa responsável por um processo, subprocesso ou atividade de negócio e cuida de todos os aspectos dos ativos de negócio, incluindo segurança, gestão, produção e desenvolvimento

2.Gerenciando os ativos de um negócio

Uma forma de controlar ou gerenciar riscos é exercer controle sobre as mudanças que representem algum tipo de risco. Esse controle pode ser feito de várias formas. Há vários modelos e métodos disponíveis que ajudam a exercer o controle. Cada um desses modelos ou métodos possui uma série de elementos básicos que ajudam no processo de controle, dos quais são:

- Entendimentos sobre como lidar com os ativos da empresa
- Entendimentos sobre como as mudanças ocorrem
- Entendimentos sobre quem pode iniciar e executar as alterações e como essas alterações serão testadas

Uma armadilha que surge ao estabelecer esses entendimentos, muitas vezes burocraticamente interpretados, é que eles podem ser elevados a um objetivo em vez de focar em seu significado.

3.Entendimento sobre como lidar com ativos de negócio

O propósito de documentar como lidar com ativos de negócio é evitar erros que possam surgir pelo uso incorreto. Uso incorreto também pode levar a um dano desnecessário. Considere, por exemplo, uma simples regra como não colocar papéis que contenham metal em um triturador de papéis. Quanto mais complexo for o ativo, mais útil será definir instruções e direções claras.

4.O uso de ativos de negócio

O uso de ativos de negócio está sujeito a certas regras. Essas regras podem ser providas em um manual e podem incluir instruções de como usar equipamentos móveis quando fora da organização. A implementação de tais regras está incluída no âmbito das medidas organizacionais.

5.Classificação da informação

Em primeiro lugar, começamos com uma explicação de alguns termos:

- A classificação é usada para definir diferentes níveis de sensibilidade na qual a informação deve ser estruturada
- Classificar é o ato de atribuir a classificação apropriada, tal como secreto, confidencial ou público, a uma informação específica. Esse termo é frequentemente usado no governo
- Designar é uma forma especial de categorizar a informação, por exemplo, de acordo com um determinado assunto da organização ou um grupo de pessoas autorizadas.
- O dono é a pessoa encarregada de um ativo de negócio.

Uma pasta na rede contendo informações pode, por exemplo, ter um dono. Se alguém deseja ter acesso a essa pasta, o dono tem que dar a permissão. O dono de um ativo de negócio

atribui uma classificação apropriada de acordo com uma lista acordada de classificações. A classificação está de acordo com a forma como o ativo de negócio é utilizado no negócio.

O dono do ativo de negócio deve assegurar que ele seja reclassificado se necessário. Se ativos e negócios de uma organização estiverem classificados, apenas o dono é capaz de reduzir a classificação ou dar permissão para que isso seja feito. A informação, por exemplo, pode ser classificada como confidencial até o momento da sua publicação, mas, uma vez que a informação tenha sido tornada pública, a classificação é reduzida.

Se um ativo possui uma classificação, é dada a ele uma marcação ou uma etiqueta. Isso pode ser colocado fisicamente e de forma visível no ativo de negócio, tal como no monitor do computador e nos cabos de transmissão, ou dentro do ativo, tal como no caso de documentos digitais, bases de dados, gravações e mensagens.

Uma medida para documentos é deixar a categoria visível em um determinado lugar do documento. Todos os documentos contendo informações restritas devem ter um número de cópia ou versão, bem como numeração de páginas. Também deve ficar claro quantas páginas o documento possui. Trata-se de uma medida bastante rigorosa, assim como deve ser possível checar cada uma das medidas.

O dono determina quem tem acesso aos ativos de negócio específicos e designados e quem não tem. A classificação de um ativo de negócio também determina como ele pode ser fisicamente armazenado. Para isso, as instalações do negócio são, às vezes, divididas em compartimentos, com requisitos de segurança diferentes para cada compartimento e crescentes níveis de segurança.

O uso de classificações é muito difícil de implementar em uma organização, uma vez que as pessoas precisam pensar com cuidado se forem aplicar classificações de forma apropriada. Outra possibilidade é não atribuir classificação a informações sigilosas. Essa informação é pública. Se o supracitado for um risco, pode ser uma política classificar toda informação como altamente sigilosa.

6.Manuseio de mídia

Mídia, refere-se a qualquer coisa em que dados possam ser gravados: papel, CDs, DVDs, pen drives, discos rígidos, fitas de backup, blackberries e outros.

O propósito de ter diretrizes sobre como manusear mídias é evitar que informações valiosas caiam em mãos erradas e prevenir as seguintes consequências: publicação não autorizada, mudanças, eliminação ou destruição de ativos ou interrupção de atividades de negócio.

A forma na qual a mídia deve ser manuseada é frequentemente ligada ao sigilo ou à classificação e é documentada em procedimentos. Após o prazo de armazenamento ter expirado, arquivos com informações sensíveis são postos em uma trituradora ou destruídos por uma empresa certificada.

7.BYOD

Em relação à propriedade de ativos, há um termo que não deve ser esquecido. Bring Your On Device (BYOD), onde as empresas dão ao seu pessoal a possibilidade de usar dispositivos próprios para trabalhar na companhia. Se esse for o caso, os ativos pessoais possuem informações de negócio e essas informações devem ser protegidas da mesma forma. Deve haver uma política para BYOD na empresa e as informações nos ativos BYOD devem ser protegidas.

Alguns pontos importantes:

- A mídia deve ser removida ou apagada de forma segura se não for mais necessária
- Manuais e documentos do sistema devem ser mantidos em local seguro e atualizados regularmente
- O transporte de mídias, que certamente estão bem embaladas, deve ser feito por uma empresa transportadora reconhecida que forneça as condições físicas corretas