1.Papéis e responsabilidades da segurança da informação

É necessário ter um sistema documentado onde os ativos e processos de segurança da informação são identificados e descritos. Todo e qualquer ativo ou processo de segurança da informação deve ser atribuído a pessoas. Essas pessoas devem ser competentes para as atribuições dadas. Além disso, a coordenação e a supervisão dos aspectos de segurança da informação referentes ao relacionamento com os fornecedores devem ser identificadas e documentadas.

É recomendável integrar papéis e responsabilidades de segurança na organização e nomear um encarregado para cada ativo, que se torna então responsável pela operação diária. O encarregado da segurança ou o gerente de segurança da informação não deve ter a responsabilidade total, mas possuir um papel consultivo junto à administração central e coordenar o processo geral de segurança da informação dentro da organização.

Dependendo do tamanho da organização, pode haver uma gama de funções ou posições para as várias responsabilidades de segurança da informação. Essas funções podem variar quanto aos títulos que lhe são dados, mas são definidas mais ou menos conforme o que segue:

- **O Chefe de Segurança da Informação (Chief Information Security Officer - CISO):** Está no mais alto nível gerencial da organização e desenvolve a estratégia geral de segurança para toda a empresa
- **O Encarregado da Segurança da Informação (Information Security Officer - ISO):** Desenvolve a política de segurança da informação de uma unidade de negócio com base na política da empresa e assegura que ela seja seguida.
- **O Gerente de Segurança da Informação (Information Security Manager - ISM):** Desenvolve a política de segurança da informação dentro da organização de TI e assegura que ela seja seguida.

Além dessas funções, que são especificamente voltadas para a segurança da informação, uma organização pode ter um Encarregado da Política de Segurança da Informação (Information Security Policy Officer) ou um Encarregado da Proteção de Dados (Data Protection Officer).

2.Separação dos deveres

Tarefas e responsabilidades devem ser separadas a fim de evitar a chance de alterações não autorizadas ou não intencionais, ou o uso indevido dos ativos da organização. Na separação dos deveres, é feita uma revisão para saber se uma pessoa realiza tomada de decisões, tarefas executivas ou de controle. Também é decidido se a pessoa precisa de acesso à informação.

O acesso sem necessidade aumenta o risco da informação ser utilizada, alterada ou destruída, intencionalmente ou não. Tão logo as funções do pessoal e as necessidades de acesso sejam definidas, as tarefas podem ser divididas, a fim de reduzir os riscos para a organização. Pode ser difícil para pequenas empresas aplicarem a separação de funções, mas esse princípio deve ser aplicado até onde for possível e prático. Quando não for prático separar adequadamente as funções, então medidas de controle alternativas devem ser investigadas e implementadas onde for possível.

3.Contato com autoridades

Contatos apropriados devem ser mantidos com as autoridades políticas locais, pessoal de apoio de emergência e provedores de serviços. As organizações devem ter procedimentos disponíveis que especifiquem quando e por quem as autoridades devem ser contatadas no caso em que leis possam ter sido quebradas. Quando sob ataque oriundo da Internet, é necessário entrar em contato com as autoridades para que sejam tomadas medidas contra a fonte do ataque. Muitos incidentes e problemas relacionados podem ter que ser classificados, e as autoridades afins listadas junto aos respectivos incidentes. Portanto, é importante manter esses detalhes à mão, uma vez que não haverá tempo para buscar essa informação quando você estiver sob alguma forma de ataque.

4.Contato com grupos de interesses especiais

A afiliação a grupos de interesse especial deve ser mantida, a fim de melhorar o conhecimento e obter acesso aos conselhos de segurança de um especialista. Busque empresas que forneçam orientações e informações sobre correções relacionadas ao hardware e ao software em uso

5.Segurança da informação e gerenciamento de projetos

Segurança da informação deve ser uma parte integral de todo projeto de uma organização e deve ser incluída na atividade de iniciação do projeto e nas suas fases subsequentes.

6.Dispositivos móveis e o trabalho remoto

O uso de equipamentos móveis tem crescido exponencialmente e possui capacidades cada vez maiores. É, portanto, aconselhável ter regras para esses equipamentos. Pense nas implicações da perda de tais dispositivos. Eles são mais do que apenas hardware; eles também contêm software e dados. Muitos dos incidentes que ocorrem envolvem equipamentos móveis. Se possível, deixe seus equipamentos móveis no trabalho; caso contrário, providencie meios adequados de armazenamento quando estiver viajando, em conjunto com um seguro.

Adote uma política de segurança que descreva técnicas, tais como rastros zero (zero footprint), tunelamento (tunneling), proteção contra malware, controle de acesso, restrição para instalação de software, registro de dispositivos, criptografia, backups, atualizações de software, fortalecimento (hardening) e treinamento de usuários. Usuários não devem usar seus dispositivos móveis em locais públicos e em outras áreas desprotegidas.

7.Trabalho remoto

O propósito de uma política de trabalho remoto é garantir que os benefícios do trabalho remoto possam ser alcançados sem aumentar indevidamente o risco aos ativos de informação da organização. Muitos dos controles de segurança existentes que são construídos de forma invisível em um ambiente de trabalho provavelmente estão ausentes em um local de trabalho remoto. Assim, eles devem ser substituídos por políticas e procedimentos adequados. A necessidade por políticas formais pode aumentar se um funcionário trabalha de casa, onde pode haver a tentação de um deslize para um estilo de comportamento doméstico em vez de profissional.

Toda organização que permite que sua equipe trabalhe remotamente só deve fazê-lo com base na avaliação do risco que isso representa. Medidas de controle apropriadas provavelmente requerem a provisão de um equipamento tanto no local da organização quanto no local remoto, particularmente para garantir a segurança adequada das comunicações.

Softwares e equipamentos devem ser licenciados e passar por manutenção: as licenças locais devem ser verificadas para assegurar se cobrem o trabalho remoto e devem ser encontrados alguns meios adequados para a manutenção do equipamento e para continuar a trabalhar se o equipamento falhar.

Também será necessário garantir que as instalações apropriadas do escritório estejam disponíveis no local do trabalho remoto: isso deve incluir pelo menos armazenamento seguro para documentos e mídias sensíveis e, possivelmente, outros equipamentos como trituradores de papel.

Embora os requisitos gerais de uma política de segurança sejam aplicados a todas as pessoas que trabalham remotamente, os riscos podem ser muito diferentes em cada caso, dependendo do local de trabalho remoto e da criticidade dos ativos de informação que o membro da equipe utilizará. Portanto, é provável que o contrato de trabalho remoto de cada indivíduo requeira a sua própria avaliação de risco, e que cada contrato seja diferente em algum detalhe.

Os quatro elementos a seguir devem ser considerados durante o desenvolvimento de uma política de trabalho remoto e oferecem sugestões de instrução para tal política:

- Autorização

- Provisão de equipamentos
- Segurança da informação durante o trabalho remoto
- Uso de equipamentos de trabalho remoto