1.O que é conformidade

Conformidade também pode ser descrita como rastreabilidade, obrigação, flexibilidade, tolerância e obediência. Resumindo, uma organização deve observar seus próprios regulamentos internos, bem como as leis do país e os requisitos da legislação e regulamentos locais. Às vezes isso pode causar conflito. Organizações multinacionais, em particular, devem aderir, por um lado, às suas próprias políticas internas, enquanto asseguram operar de forma consistente fazendo o mesmo em relação à legislação e aos regulamentos locais e internacionais.

1.1 Medidas de conformidade

Como resultado do que foi exposto, fica claro que produzir uma política interna dentro de uma organização é a maneira de entrar em conformidade. O primeiro passo para uma organização é produzir uma política declarando que deve cumprir a legislação e local, bem como os regulamentos. Além disso, devem ser desenvolvidos procedimentos, diretrizes e ferramentas que esclareçam e ajudem os funcionários a aplicar esses regulamentos na prática.

Análise de riscos devem ser conduzidas para garantir que os riscos relevantes sejam identificados, os níveis corretos de segurança sejam estabelecidos e sejam determinadas e implementadas as medidas apropriadas para esses níveis de segurança. Conformidade está relacionada com a área de segurança, mas é um campo especializado do conhecimento. Para alcançar a conformidade, é importante trabalhar em estreita colaboração com especialistas legais.

1.2 Observância das disposições legais

O principal propósito de toda empresa é atingir seus próprios objetivos de negócio. Isso significa desenvolver um determinado produto fornecer certos serviços. Todas as empresas, no entanto, devem observar a legislação local, os regulamentos e as obrigações contratuais. Os requisitos de segurança que uma empresa deve cumprir estão fortemente relacionados a isso.

Embora a legislação e os regulamentos locais sejam aderentes aos acordos internacionais, isso não significa que eles sejam projetados para apoiar empresas que operam internacionalmente. Essas empresas necessitam de uma política de alto nível que, de alguma forma, seja mais geral, cujos documentos de política decorrentes devem ser adaptados à legislação em vigor no país em que estão situadas, para que façam negócios localmente. Os requisitos legais podem diferir um pouco, particularmente no campo da privacidade e, portanto, a maneira como se lida com informações que podem envolver privacidade também deve ser diferente.

Para assegurar que os requisitos legais e regulatórios sejam observados, é sempre importante buscar aconselhamento de assessores jurídicos da organização ou de advogados qualificados. Não há uma solução única para tudo quando se trata de regulamentações.

Regulamentações governamentais são geralmente específicas de cada país e podem conter regras de segurança para informações especiais. Informação especial é um termo utilizado para informações que precisam de proteção extra, com base na natureza sensível que decorre de seu potencial impacto ou risco para a segurança nacional.

1.3 Direitos de propriedade intelectual

Quando uma empresa usa software, a utilização de material que pode estar sujeito a direitos de propriedade intelectual (IPR) deve ser abordada. As diretrizes listadas a seguir precisam ser consideradas, a fim de proteger o material que pode ser considerado propriedade intelectual.

É importante entender que o material protegido por direitos autorais também precisam ser abordado, para garantir o cumprimento da legislação sobre de direitos autorais vigente no país, você deve:

- Publicar uma política referente à conformidade em relação aos direitos de propriedade intelectual, onde é definido o uso legal de programas de computadores e de informações.
- Manter uma política de conscientização para a proteção dos direitos de propriedade intelectual; incluir na política de IPR as medidas disciplinares que a organização irá tomar em relação a qualquer funcionário que viole essa política
- Reconhecer que os direitos de propriedade intelectual incluem os direitos autorais de programas de computador, documentos, direitos de design, marcas comerciais, patentes e licenças de código-fonte.
- Somente comprar programas de computador de fornecedores bem conhecidos e renomados para garantir que nenhum copyright seja infringido
- Assegurar que, se for utilizado código aberto, o respectivo formulário de licença deve ser respeitado e observado
- Manter um registro dos ativos e identificar todos os requisitos associados a esses ativos em relação à proteção dos direitos de propriedade intelectual
- Compreender que os programas de computadores que estão sujeitos a direitos de propriedade intelectual são normalmente fornecidos com base em um contrato de licença o qual estabelece as condições da licença.

1.4 Protegendo dados e a confidencialidade de informações pessoais

A proteção dos dados e da privacidade recai sob a legislação e as diretrizes de proteção de dados pessoais. Além disso, cláusulas contratuais com um cliente podem desempenhar esse papel. Toda organização deve ter uma política de proteção de dados pessoais e essa política deve ser conhecida de todos os que processam esses dados. A observação dessa política e de toda a legislação e os regulamentos relevantes para a proteção de dados pode, muitas vezes, ser mais bem alcançada se for designada uma pessoa especificamente responsável pela proteção dos dados e que dê suporte a gerentes, usuários e provedores de serviço na execução de suas funções nessa área.

1.5 Proteção de registros

As ferramentas utilizadas para auditoria de sistemas devem ser mantidas separadas dos sistemas de desenvolvimento e dos sistemas de produção e não devem ser armazenadas em bibliotecas de fitas ou salas de usuários, a não ser que tenham sido tomadas medidas de proteção adicionais de nível adequado. Se terceiros são envolvidos em uma auditoria, existe o risco das ferramentas de auditoria e as informações a que este terceiro tem acesso serem mal utilizadas. Medidas como limitar o acesso a apenas os sistemas de que o auditor necessita para sua investigação, um acordo de não divulgação e limitar o acesso físico podem ser consideradas para ajudar a mitigar esse risco. Uma vez concluída a auditoria, a organização deve alterar imediatamente as senhas que foram dadas aos auditores.

2.Revisões de segurança da informação

Revisões são úteis como um meio de avaliar periodicamente medidas, processos e procedimentos de segurança. Dependendo do escopo de uma revisão, ela pode ser usada para diferentes propósitos. As revisões podem ser aplicadas para testar se as medidas de segurança estão em conformidade com requisitos definidos, tais como normas da empresa, leis e regulamentos. São aplicadas para avaliar se as medidas de segurança estão alinhadas com os requisitos de conformidade específicos identificados para um sistema de informação, e se essas medidas foram implementadas e são mantidas de forma eficaz. As revisões também ajudam a verificar se essas medidas estão funcionando conforme especificado e esperado.

A fim de garantir que a importância das revisões seja abordada de forma suficiente, elas devem fazer parte de um programa de revisão. Os elementos de um programa de revisão incluem, dentre outras coisas, o escopo, o critério, a frequência e as metodologias de revisão. O plano deve indicar quais áreas precisam ser revisadas juntamente com os resultados de revisões anteriores.

É importante prestar atenção à seleção dos auditores, uma vez que eles precisam ser objetivos para garantir a imparcialidade do processo de revisão. Uma regra de ouro é que um auditor nunca deve revisar seu próprio trabalho. É necessário um procedimento documentado que descreva as responsabilidades dentro de um escopo para definir o planejamento, e a condução, das revisões.

O gerente responsável deve garantir que quaisquer não conformidades identificadas sejam tratadas e suas causas investigadas. Além disso, deve garantir que todas as ações necessárias sejam tomadas e verificar os resultados dessas ações. Finalmente, o auditor interno e/ou externo deve verificar se a organização cumpre os regulamentos. O auditor faz isso examinando se uma medida específica está em vigor.

2.1 Conformidade com políticas e padrões de segurança

Existem muitas organizações e padrões sobre segurança da informação. Padrões importantes desenvolvidos pela ISO, NIST e ANSI. Na Europa, a ISO é a mais utilizada, já nos EUA, os padrões NIST e ANSI são mais comuns.

A ISO, fundada em 1974, é uma federação mundial de organismos nacionais de normatização de cerca de 100 países, com um organismo de normalização representando cada país membro. As organizações membro colaboram com o desenvolvimento e a promoção de padrões internacionais. Dentre os padrões que a ISO promove está a Interconexão de Sistemas Abertos (OSI), um modelo de referência para protocolos de comunicação.

NIST é uma unidade do Departamento de Comércio dos EUA. A série NIST 800 é um conjunto de documentos que descreve políticas, procedimentos e diretrizes para a segurança de computadores do governo federal dos EUA. Os documentos estão disponíveis de graça e podem ser úteis para instituições de negócio e de educação, bem como para agências do governo. As publicações da série NIST 800 evoluíram como resultado de uma pesquisa exaustiva sobre métodos viáveis e econômicos para otimizar, de forma proativa, a segurança dos sistemas e redes de tecnologia da informação (TI). As publicações abrangem todos os procedimentos e critérios que o NIST recomenda para avaliar e documentar ameaças e vulnerabilidades e para implementar medidas de segurança, a fim de minimizar o risco de eventos adversos. As publicações podem ser úteis como diretrizes para a aplicação de regras de segurança e como referências legais no caso litígio envolvendo questões de segurança.

O ANSI é a principal organização para fomento do desenvolvimento de padrões de tecnologia nos Estados Unidos. O ANSI trabalha com grupos da indústria e é membro dos EUA na ISO e na Comissão Internacional de Eletrônica (IEC). Padrões de computador estabelecidos há muito tempo pela ANSI incluem o Código Americano Padrão para Intercâmbio de Informações (ASCII), e a Pequena Interface para Sistemas de Computador (SCSI).

ITU-T é o principal organismo internacional para a promoção de padrões cooperativos para equipamentos e sistemas de telecomunicações. Era anteriormente conhecida como CCITT e está localizada em Genebra, na Suíça.

IEEE se descreve como “a maior sociedade técnica profissional do mundo - promovendo o desenvolvimento e a aplicação de tecnologias elétricas e das ciências afins para o benefício da humanidade, o avanço da profissão e o bem-estar dos nossos membros”. O IEEE promove o desenvolvimento de padrões que muitas vezes se tornam padrões nacionais e internacionais. A organização pública diversos periódicos, possuir muitas seções locais e várias grandes sociedades em áreas especiais. Os protocolos mundialmente utilizados para a conexão de redes sem fio se baseiam em tecnologias IEEE, como as versões IEEE 802.11a, 802.11b, 802.11g, 802.11n e a nova 802.11ac, para prover conectividade sem fio, bem como os padrões de criptografia WEP e WPA.

OWASP é um projeto de segurança de aplicativos de código aberto. A comunidade OWASP inclui corporações, organizações educacionais e indivíduos de todo o mundo. Essa comunidade trabalha para criar artigos, metodologias, documentações, ferramentas e tecnologias disponibilizados de graça. A fundação OWASP é uma organização de caridade

que apoia e gerencia projetos e infraestruturas OWASP. Ela não é afiliada a nenhuma empresa de tecnologia, embora apoie o mencionado uso de tecnologias de segurança. O OWASP tem evitado se afiliar, pois acredita que a ausência de pressões organizacionais pode facilitar a prestação de informações imparciais, práticas econômicas sobre a segurança das aplicações. O OWASP defende a abordagem da segurança de aplicativos levando em conta as dimensões, processos, pessoas e tecnologia.