Estudo de auditoria de segurança da informação

Fabiana Cristina de Sousa[1], Millys Fabrielle Araújo Carvalhaes[2]

[1,2]Bacharelado em Engenharia de Computação – Centro Universitário de Anápolis (UniEVANGÉLICA) – Anápolis - GO

[1]fabi_sousa1995@hotmail.com, [2]millys.carvalhaes@docente.unievangelica.edu.br

Resumo. *Auditoria de segurança é uma técnica de avaliação sistemática em mensurável da política de segurança de uma organização aplicada a um local específico. Faz parte do processo definir e manter uma política de segurança da informação efetiva. Envolvendo todas as pessoas que utilizam algum recurso computacional através de uma organização.*

1. Introdução

Hoje estamos em um mundo tecnológico de constante crescimento e inovação, informações que antes eram anexadas em papeis ou conhecimento das pessoas, hoje são passadas para o mundo digital, garantindo facilidade de acesso compartilhamento com outras pessoas em qualquer parte do mundo.

Existem diversas formas de disponibilizar uma informação, mas nem toda informação é pública. Muitas informações, depende de regras e políticas empresariais ou pessoais, por serem privadas e somente poderão ser acessadas quando tais regras foram cumpridas.

Auditoria de segurança é uma técnica de avaliação sistemática em mensurável da política de segurança de uma organização aplicada a um local específico. Faz parte do processo definir e manter uma política de segurança da informação efetiva. Envolvendo todas as pessoas que utilizam algum recurso computacional através de uma organização.

2. Sistema de Gestão de Segurança da Informação

Este processo torna uma informação pública em privado é executado dento do ramo da Segurança da Informação, cuja a importância hoje é externa.

Visando tornar os sistemas de informação mais seguros e confiáveis, agregando valor ao negócio. Como parte do seu ciclo de planejamento, existem os denominados Sistemas de Gestão de Segurança da Informação (SGSI), que garante que a segurança da informação seja eficaz e eficiente.

Entretanto é um trabalho árduo, que envolve toda governança de TI, utilizando as melhores práticas do COBIT, ITIL, COSO, dentre outros sendo essencial para que a segurança de da informação seja confiável, precisa segurança atualizada e integra. O alto nível de governança não designado somente a empresas grandes, mas também para as médias e pequenas empresas, tendo seus processos bem definidos e seguindo ao menos os princípios básicos da implantação de tal governança, pensando principalmente que a mesma deve estar em total sintonia com os objetivos do negócio da empresa e respondendo a Governança Corporativa.

Existem vários aspectos a serem considerados sobre a implantação de um sistema de gestão de Segurança da Informação como:

A leis Sarbanes Oxley, denominada também de SOX que implica um processo de auditoria eficaz, garantindo que as informações financeiras, de importância, estejam completamente seguras, integras e sem a possibilidade de haver fraude.

Além de serem informações importantes tanto em uma organização como para um pessoal é um dos principais fatos de ataques de crackers e outros indivíduos.

Para isso além da SOX utiliza a Committee of Spondoring Organizations of the Treadway (COSO) que é o Comitê das Organizações Patrocinadoras que auxilia no controle de riscos nos sistemas de informação e fraudes em relatórios financeiros. Com as auditorias propostas pelo COSO pode-se garantir mais confiabilidade dos sistemas de informação e garantia de reconhecimento internacional, devido aos padrões de alta qualidade e segurança adquiridos em tal sistema.

3. Normas e Certificações

Outro aspecto de total importância é a aquisição de certificação ISO que é a organização que provê normas em geral mundialmente, entre estas normas destacamos a ISO/ICE 27001 e ISO/ICE 27002.

A ISO/ICE 27001 É a norma internacional que define os Requisitos para Sistemas de Gestão de Segurança da Informação. Ela ajuda a empresa a adotar um sistema de gestão da segurança da Informação que permita mitigar os riscos de segurança atribuídos a seus ativos e adequar as necessidades a área de negócio.

3.1. Alguns benefícios propostos pela Norma ISO 27001

- Reduz o risco de responsabilidade pela não implementação ou determinação
- de políticas e procedimentos
- Oportunidade de identificar e corrigir pontos fracos
- A alta direção assume a responsabilidade pela segurança da informação
- Permite revisão independente do sistema de gestão da segurança da
- informação
- Oferece confiança aos parceiros comerciais, partes interessadas, e clientes
- Melhor conscientização sobre segurança
- Combina recursos com outros Sistemas de Gestão
- Mecanismo para se medir o sucesso do sistema

3.2. Estrutura da Norma ISO 27001

1. Introdução
2. Objetivo
3. Referência normativa
4. Termos e definições
5. Sistema de gestão de segurança da informação
6. Responsabilidade da direção
7. Auditorias internas do SGSI
8. Análise crítica do SGSI pela direção
9. Melhoria do SGSI

A certificação ISO 27001 pode ser obtida por empresas e não por profissionais. A ISO/ICE 27002 é recomendável que a ISO 27001 seja utilizada em conjunto com a 27002, que é um código de práticas com um conjunto completo de controles que auxiliam aplicação

do Sistema de Gestão da Segurança da Informação, facilitando atingir os requisitos especificados pela Norma ISO 27001.

A ISO 27002 fornece um conjunto de Controles baseados em melhores práticas para a Segurança da Informação. Ela não deve ser utilizada em auditorias mas simplesmente servir como um guia. A Norma está dividida em 11 capítulos. Ao contrário da ISO 27001, a certificação ISO 27002 pode ser obtida por profissionais. Ela corresponde a antiga certificação ISO 17799.

4. Auditoria de Sistemas de Informação

De grande relevância na área de Segurança da Informação é o processo de auditoria de sistemas de informação.

A auditoria visa garantir que a qualidade de um Sistema de informação em relação a Segurança da informação, esteja em um alto nível e solidificado com normas e governança de TI eficaz.

O auditor deve possuir uma vasta experiência no assunto e sempre atualizado com relação a novas tendências, processos, legislação e normas a fim de poder exercer com eficácia sua profissão e ajudar a empresas a tomar o rumo da confiabilidade professional.

Os processos internos de TI devem passar por auditorias planejadas, visando não somente encontrar problemas e verificar conformidades, mas assegurar planos de contingência contra possíveis riscos e incidentes. A auditoria interna possui não somente o papel de auditor, como propriamente, mas de alertar e ajudar na busca por soluções eficazes que garantam a continuidades do negócio da organização.

A análise de riscos de TI é um processo interno da auditoria importante, pois é possível prever problemas futuros, analisar a probabilidade de ocorrências dos mesmos, como também analisar o impacto de que irá causar na organização, caso venha acontecer, e tomar decisões de contingência e mitigação.

5. Conclusão

Em geral, a Segurança da informação, quando bem implementada, auditada e certificada, agrega um enorme valor ao negócio. O processo é árduo e custoso, mas os benefícios são muito maiores e o future é garantido. É de extrema importância estarmos preparados para trabalhar com a Segurança da informação alinhados aos negócios da empresa, ou aos objetivos pessoais quando se tratando de informações pessoais.

Referências

ISO 27001 e ISO 27002 (2017). https://www.portalgsti.com.br/2011/05/iso-27001-e-iso-27002.Junho.

Segurança da Informação e Auditoria de Sistemas da Informação (2017). http://www.blogdobsi.com/2015/10/19/seguranca-da-informacao-e-auditoria-de-sistemas-de-informacao/. Junho

Clavis (2017). Teste de Invasão. http://www.clavis.com.br/servico/auditoria-redes-e-sistemas.php. Junho.