Universidade nove de julho

Diretoria dos cursos de informática

NOME: Matheus Henrique Natal de Souza
RA: 318103322

NOME: Reginaldo José Aparecido
RA: 318103339

NOME: Weverton de Lima Oliveira
RA: 318105267

Projeto de infraestrutura em TI

MRW technology

São Paulo
01/12/2018

NORMA DE BOAS PRÁTICAS

ISO 27055: Boas práticas para gestão de segurança da informação

Segurança da informação é um tema que ganhou corpo nos últimos anos, obtendo espaço nas mídias e tornando-se “commodity”, em empresas dos mais variados portes e segmentos. Em contrapartida é importante frisar que a popularização do termo SI (Segurança da Informação) foi motivada pela elevação no número de incidentes de segurança, ocorridos em âmbito mundial. Os transtornos gerados por estes incidentes são variados gerando, desde danos a imagem do negócio, vazamento de informações críticas, podendo acarretar em perdas financeiras substanciais.

O aumento do número de ocorrências influência na percepção de valor sobre investimentos em SI, e fazem com que empresas busquem a estruturação de processos para garantir que seus negócios estejam protegidos contra os mais variados tipos de ameaças virtuais.

Em meio a este cenário, surgiu a norma internacional NBR ISO/IEC 27055, que foca nas boas práticas para a gestão da segurança da informação. Nos dias de hoje, ela é fundamental para a consolidação de um Sistema de Gestão de Segurança da Informação (SGSI), garantindo a continuidade e manutenção dos processos de segurança, alinhados aos objetivos estratégicos da organização. A seguir, conheça as principais características da norma, bem como os benefícios associados a sua implantação:

O que é a ISO 27055?

Em 1995, as organizações internacionais ISO (The International Organization for Standardization) e IEC (International Electrotechnical Commission) deram origem a um grupo de normas que consolidam as diretrizes relacionadas ao escopo de Segurança da Informação, sendo representada pela série 27000. Neste grupo, encontra-se a ISO/IEC 27055, norma internacional que estabelece código de melhores práticas para apoiar a implantação do Sistema de Gestão de Segurança da Informação (SGSI) nas organizações.

Através do fornecimento de um guia completo de implementação, ela descreve como os controles podem ser estabelecidos. Estes controles, por sua vez, devem ser escolhidos com base em uma avaliação de riscos dos ativos mais importantes da empresa. Ao contrário do que muitos gestores pensam, a ISO 27055 pode ser utilizada para apoiar a implantação do SGSI em qualquer tipo de organização,

pública ou privada, de pequeno ou grande porte, com ou sem fins lucrativos; e não apenas em empresas de tecnologia.

Quais seus objetivos?

O principal objetivo da ISO 27055 é estabelecer diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão de segurança da informação em uma organização. Isso também inclui a seleção, a implementação e o gerenciamento de controles, levando em conta os ambientes de risco encontrados na empresa.

ISO 27055, benefícios para as empresas?

As vantagens proporcionadas pela certificação ISO 27055 são representativas para as empresas, principalmente pelo fato de serem reconhecidas mundialmente. Conheça alguns benefícios associados a aplicação da norma:

- Melhor conscientização sobre a segurança da informação;
- Maior controle de ativos e informações sensíveis;
- Oferece uma abordagem para implantação de políticas de controles;
- Oportunidade de identificar e corrigir pontos fracos;
- Redução do risco de responsabilidade pela não implementação de um SGSI ou determinação de políticas e procedimentos;
- Torna-se um diferencial competitivo para a conquista de clientes que valorizam a certificação;
- Melhor organização com processos e mecanismos bem desenhados e geridos;
- Promove redução de custos com a prevenção de incidentes de segurança da informação;
- Conformidade com a legislação e outras regulamentações.
-

Quais os principais itens que compõem o ISO 27055?

A parte principal da norma se encontra distribuída nas seguintes seções, que correspondem a controles de segurança da informação. Vale lembrar que a organização pode utilizar essas diretrizes como base para o desenvolvimento do SGSI. Sendo elas:

Seção 5 – Política de Segurança da Informação

Deve ser criado um documento sobre a política de segurança da informação da empresa, que deve conter os conceitos de segurança da informação, uma estrutura

para estabelecer os objetivos e as formas de controle, o comprometimento da direção com a política, entre tantos outros fatores.

Seção 6 – Organização da Segurança da Informação

Para implementar a Segurança da Informação em uma empresa, é necessário estabelecer uma estrutura para gerencia-la da maneira adequada. Para isso, as atividades de segurança da informação devem ser coordenadas por representantes da organização, que devem ter responsabilidades bem definidas e proteger as informações de caráter sigiloso.

Seção 7 – Gestão de ativos

Ativo, segundo a norma, é qualquer coisa que tenha valor para a organização e que precisa ser protegido. Mas para isso, os ativos devem ser identificados e classificados, de tal forma que um inventário possa ser estruturado e posteriormente mantido. Além disso, eles devem seguir regras documentadas, que definem qual o tipo de uso é permitido fazer com esses ativos.

Seção 8 – Segurança em recursos humanos

Antes de realizar a contratação de um funcionário – ou mesmo de fornecedores – é importante que ele seja devidamente analisado, principalmente se for lidar com informações de caráter sigiloso. A intenção desta seção é mitigar o risco de roubo, fraude ou mau uso dos recursos. E quando o funcionário estiver trabalhando na empresa, ele deverá estar ciente das ameaças relativas à segurança da informação, bem como de suas responsabilidades e obrigações.

Seção 9 – Segurança física e do ambiente

Os equipamentos e instalações de processamento de informação críticas ou sensíveis devem ser mantidas em áreas seguras, com níveis e controles de acesso apropriados, incluindo proteção contra ameaças físicas e ambientais.

Seção 10 – Segurança das operações e comunicações

É importante que estejam definidos os procedimentos e responsabilidades pela gestão e operação de todos os recursos de processamento das informações. Isso inclui o gerenciamento de serviços terceirizados, o planejamento dos recursos dos sistemas para minimizar o risco de falhas, a criação de procedimentos para a geração de cópias de segurança e sua recuperação e a administração segura de redes de comunicações.

Seção 11 – Controle de acesso

O acesso à informação, assim como aos recursos de processamento das informações e aos processos de negócios, deve ser controlado com base nos requisitos de negócio e na segurança da informação. Deve ser assegurado o acesso de usuário autorizado e prevenir o acesso não autorizado a sistemas de informação, a fim de evitar danos a documentos e recursos de processamento da informação que estejam ao alcance de qualquer um.

Seção 12 – Aquisição, desenvolvimento e manutenção de sistemas

Os requisitos de segurança de sistemas de informação devem ser identificados e acordados antes do seu desenvolvimento e/ou de sua implementação, para que assim possam ser protegidos visando a manutenção de sua confidencialidade, autenticidade ou integridade por meios criptográficos.

Seção 13 – Gestão de incidentes de segurança da informação

Procedimentos formais de registro e escalonamento devem ser estabelecidos, e os funcionários, fornecedores e terceiros devem estar conscientes sobre os procedimentos para notificação dos eventos de segurança da informação, para assegurar que eles sejam comunicados o mais rápido possível e corrigidos em tempo hábil.

Seção 14 – Gestão da continuidade do negócio

Planos de continuidade do negócio devem ser desenvolvidos e implementados, visando impedir a interrupção das atividades do negócio e assegurar que as operações essenciais sejam rapidamente recuperadas.

Seção 15 – Conformidade

É importante evitar a violação de qualquer lei criminal ou civil, garantindo estatutos, regulamentações ou obrigações contratuais e de quaisquer requisitos de segurança da informação. Caso necessário, a empresa pode contratar uma consultoria especializada, para que verifique sua conformidade e aderência a requisitos legais e regulamentares.