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 prevenido 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.