

SECURITY OFFICER

A importância do profissional de Segurança da Informação nas instituições

O Security Officer é o profissional responsável pela Segurança da Informação de uma instituição. E o que é Segurança da Informação (SI)? Qual a importância de designar uma pessoa especialmente para esta área?

Primeiramente, deve-se visualizar o seguinte cenário: atualmente vive-se em uma sociedade totalmente dependente de tecnologia, onde a inclusão digital cresce exponencialmente. Logo, as informações, antes armazenadas em papéis e arquivos gigantescos, concentram-se cada vez mais em dados, resumindo-se a bits armazenados em microchips. O principal ativo das instituições é a informação.

As informações, agora digitais, são criadas, processadas, armazenadas e transportadas em dispositivos eletrônicos. É possível conectarmos um *pendrive* a um computador e copiarmos todo o banco de dados de uma empresa em poucos minutos. Ou pode-se também levar diversos documentos sigilosos, notas fiscais e outras informações impressas.

Mas será que quem fez essa cópia tinha autorização para tanto? Quais informações foram apropriadas indevidamente ou “deletadas”? Qual será o destino desses arquivos?

Neste cenário, cabe à organização definir quais são as regras e condutas esperadas de seus colaboradores por meio de políticas e normas, e implementar controles de segurança em seus ativos de informação¹.

Para implementar segurança nos procedimentos de uma instituição, garantindo-lhe que seus ativos estarão protegidos, e conseqüentemente, que estará resguardada a reputação e imagem da empresa, a presença de um *Security Officer* é extremamente útil. Ele irá gerir todas as atividades de uma instituição relacionadas à Segurança da Informação.

E por Segurança da Informação, conforme a ABNT NBR ISO/IEC 27002:2005, entendemos que é a proteção da informação de vários tipos de ameaças, a fim de garantir a continuidade do negócio, minimizar os riscos, maximizar o retorno sobre os investimentos e as

¹ Segundo Marcos Sêmola: “a informação representa a inteligência competitiva dos negócios e é reconhecida como ativo crítico para continuidade operacional e saúde da empresa”. (in “Gestão da Segurança da Informação: uma visão executiva”, Ed. Campus, 2002, 7ª ed.). Site: www.semola.com.br

oportunidades para a instituição. Segurança da Informação consiste na proteção dos ativos que contêm informações, isto é, ativos que geram, processam, manipulam, transmitem e armazenam informações.

A Segurança da Informação garante que os ativos da instituição sejam protegidos sob três requisitos:

- **Confidencialidade:** é o sigilo da informação. Garantia de que apenas as pessoas que devem ter conhecimento a seu respeito poderão acessá-la.
- **Integridade:** garantia de que as informações irão permanecer em seu estado original, protegida de alterações.
- **Disponibilidade:** garantia de que as informações estarão acessíveis àqueles que dela necessitam, no momento em que precisam.

A criação de uma área específica de Segurança da Informação facilita a implantação de mecanismos de proteção contra as vulnerabilidades físicas, lógicas e comportamentais, que tanto afetam as instituições.

Eliminando-se (ou administrando-se) tais ameaças, diminui-se eventual impacto negativo nos negócios, na imagem e na reputação da empresa, bem como se resguarda os clientes desta contra riscos iminentes ou futuros.

De tal modo, o *Security Officer* agrega um diferencial competitivo à instituição, através de gestão de riscos e implantação de controles, viabilização de novos negócios e governança de Segurança da Informação.

O *Security Officer* terá sua atuação vinculada à área de SI da instituição, ou mesmo a um Comitê de SI, sendo independente do Departamento de TI e reportando-se à Diretoria da empresa. Deverá atuar sempre tendo em mente os “4 P’s da Segurança”: Pessoas, Políticas, Processos e Produtos; atentando aos objetivos e características específicas do negócio, aos aspectos legais e normativos (*compliance*), bem como à infra-estrutura física da organização.

Apesar de ser comum que responsáveis da área de TI atuem no departamento de Segurança da Informação concomitantemente, isto não é recomendável. Profissionais responsáveis por TI e SI, atuando em ambas as áreas, criam situações de conflitos de

interesses, afinal, o profissional de SI é responsável por verificar também a área de TI. E neste caso, como um mesmo indivíduo poderá fiscalizar-se a si próprio?!

O *Security Officer* deverá agir com imparcialidade e autonomia, por isso o ideal é que esteja atrelado exclusivamente à área de SI, e que esta não seja subordinada a TI.

O profissional de Segurança da Informação terá também uma grande responsabilidade: conscientizar os usuários, visto que de nada adianta implantar políticas, normas e procedimentos, adquirir ferramentas tecnológicas, se os indivíduos não têm consciência sobre o uso das tecnologias. Afinal, *“segurança é um processo, não um produto.”*²



Gisele Truzzi

Advogada especialista em Direito Digital e Direito Criminal

www.truzzi.com.br

gisele@truzzi.com.br

² SCHNEIER, Bruce. Renomado especialista em segurança computacional e criptografia, autor de vários livros sobre o assunto, tais como *“Applied Cryptography”*, *“Secrets and Lies”*, *“Beyond Fear”* e *“Schneier on Security”*. Site: www.schneier.com.