Fabio Sobiecki

Conformidade na Segurança da Informação

O que é Conformidade?

Conformidade é o ato de estar conforme uma regra ou lei

Leis:

- Lei Geral de Proteção de Dados
- Marco Civil Regulatório

Normas:

- ISO 27001, NIST, PCI/DSS

Políticas de Segurança

A política, é uma definição por escrito, de regras que devem ser seguidas pelos envolvidos, visando aumentar a segurança.

Política de Senha

Política de Backup

Política de Segurança

Normas da Segurança

As normas são um conjunto de regras, estabelecida por uma empresa, entidade, corpo de profissionais, que tem como objetivo o aumento na segurança.

Também chamada de “melhores práticas”

Surgiu da experiência de outras empresa

Em alguns casos, tem uma forte recomendação

Leis e Regulação

A empresa se sujeita as leis municipais, estaduais, federais de onde está registrada.

Na Internet, se tem relações comerciais com outros países, deve observar as leis dos países de onde o consumidor reside.

As leis são obrigações mandatórias, portanto, devem ser priorizadas na gestão de segurança.

Assessment e Auditoria

Como você pode avaliar sua empresa, quanto às práticas de segurança.

Um assessment avalia sua empresa, através de uma visão externa e comparativa com outras empresas do setor.

Auditoria, normalmente associada à conformidade, avalia se sua empresa atende aos requisitos de conformidade.

Auditoria Interna e Externa

Auditoria Externa é feita por uma empresa de consultoria ou auditoria. Tem auditores independentes, que não possuem conflito de interesse.

Aplicada em avaliações legais, empresas que tem ações na bolsa de valores ou companhias S.A.

Auditoria Interna avalia questões diárias, apoia a área de segurança em projetos e recomendações e avalia políticas e regulações internas.

Resumo

- O que é Conformidade
- Políticas de Segurança
- Normas de Segurança
- Leis e Regulações
- Assessment vs. Auditoria
- Auditoria Interna e Externa

Outras demandas da área

O que mais a área de GRC cuida?