

TRIBUNAL DE JUSTIÇA DO DISTRITO FEDERAL E DOS TERRITÓRIOS

CARGO 15: TÉCNICO JUDICIÁRIO – ÁREA: APOIO ESPECIALIZADO ESPECIALIDADE: PROGRAMAÇÃO DE SISTEMAS

PROVA DISCURSIVA
APLICAÇÃO: 20/12/2015

PADRÃO DE RESPOSTA DEFINITIVO

Genericamente, uma política de segurança da informação é um conjunto de leis, regras e práticas que regulamentam como a organização deve gerenciar, proteger e distribuir a informação que manuseia, de modo seguro.

Esse arcabouço normativo deve variar de organização para organização, visto que em cada uma a informação tem seu valor próprio, sua importância para os negócios e até o seu grau de criticidade para sobrevivência da organização. Aspectos como o modelo de gestão, a cultura organizacional, o caráter competitivo, a conduta ética e a maturidade de processos também afetam as políticas de segurança da informação.

As políticas de segurança da informação são entidades que vêm dar estrutura formal à iniciativa de proteger a informação organizacional, ou seja, de promover a segurança da informação. Por sua própria natureza, devem prescrever pela preservação da confidencialidade, pela integridade e pela disponibilidade da informação, em níveis razoáveis e adequados ao negócio da organização e a seu alinhamento estratégico.

Normalmente, as políticas de segurança são representadas por um documento principal que trata das questões de segurança da informação numa abordagem mais gerencial, mais estratégica, e de outros documentos subordinados, com regras mais específicas, além de textos voltados a procedimentos operacionais, em nível bastante detalhado e intrinsecamente ligado ao cotidiano funcional da organização. Estes últimos documentos são os mais mutáveis, e podem variar a cada mudança de tecnologia, a cada ajuste interno, ou diante de conjunturas externas de influência. Os documentos de regras podem ter outras políticas, voltadas ao tratamento de temas específicos, como política de controle de acesso, política de backup, política de uso aceitável dos recursos de TI, política de privacidade, política de senhas, entre outras.

Uma das características mais importantes das políticas de segurança da informação é a de que elas precisam ser chanceladas pela alta direção da organização, para que atinjam todos os níveis e colaboradores e possam ter o efeito esperado sobre os cuidados com as informações de toda a organização. A despeito desse caráter oficial e abrangente, várias dificuldades na implementação e no cumprimento de políticas de segurança da informação organizacionais sugerem que seus modelos conceituais não são tão ajustados quanto precisariam ser. Parte desse problema pode ser atribuída à conceituação e visão local da segurança da informação, à falta de maturidade em gestão, à dimensão relativa na classificação e valoração das informações da organização, e à baixa consideração da importância dos usuários da informação na construção e definição das políticas, em contraponto à importância atribuída normalmente aos aspectos tecnológicos.

Por fim, mesmo com as imperfeições e limitações das políticas de segurança da informação, o que reflete a ineficiência das organizações em se reconhecer claramente, é possível dizer que elas funcionam como uma pedra angular das organizações, sendo referência para o que se pretende e o que efetivamente se realiza em termos de proteção à informação nas organizações.