Por Edison Franco

Em tempos atuais de turbulências corporativas, a questão do Compliance (conformidade com a legislação e comportamentos definidos) tem sido mais fortemente debatida. Em relação ao recurso informação, para se estar em Compliance é fundamental a existência de um Processo Corporativo de Segurança da Informação. Compliance não acontece sem a segurança da informação! A segurança da informação é a base para um processo de Compliance Corporativo.

Mas, como desenvolver uma Gestão de Compliance da Informação? Descrevemos abaixo as etapas necessárias para que uma organização desenvolva e mantenha a sua informação ou a informação que está sob sua responsabilidade, de maneira adequada aos requisitos de conformidade exigidos.

1. Identifique seus direcionadores

Inicialmente, para realizar uma Gestão de Compliance da Informação, é necessário identificar quais são os direcionadores obrigatórios que a organização precisa seguir, precisa estar em conformidade, isto é, precisa estar em Compliance.

Definimos como Direcionadores Obrigatórios:

– Legislação (nacional ou de outros países).

– Regulamentos específicos de um determinado segmento (exemplo das instituições financeiras).

– Exigências de mercado (pode ser uma certificação).

– Regras definidas pela própria organização, como Código de Conduta, Código de Ética, Código de Transparência da Informação.

– Algum elemento específico para a organização.

Exceto em relação à legislação e regulamentos setoriais que todas as organizações são obrigadas a cumprir, os demais direcionadores vão depender do que a organização deseja. Sendo assim, estar em conformidade pode ser diferente para organizações diferentes. O exemplo mais simples é o Código de Conduta. Apesar de todas as organizações possuírem um belo e exemplar texto, o que vale na prática é a prática do Código de Conduta.

2. Identifique quais são os controles exigidos pelos direcionadores

Cada direcionador define uma série de controles que devem ser desenvolvidos, implementados e mantidos (sustentados) ao longo do tempo pela organização. Algumas definições são amplas e bem conceituais, dando margem a várias interpretações para a sua implementação. Outras definições, por sua vez, são bastante específicas e de fácil verificação o seu funcionamento.

Para os controles mais conceituais, explicite o que significa seguir estes controles. É necessário que toda a organização e principalmente o seu Corpo Diretivo entenda e esteja ciente das consequências do atendimento a estes controles.

3. Defina uma Arquitetura de Segurança da Informação

Para a existência de um Processo Corporativo de Segurança da Informação é necessário um passo anterior: a definição de qual arquitetura iremos seguir. Existem diversas arquiteturas e cada uma com suas características. Pessoalmente entendo que a arquitetura definida pela Norma NBR

ISO/IEC 27002 é um padrão aceito internacionalmente e de fácil entendimento. Além de já ser uma norma ABNT e de fácil acesso para todas as organizações. Mas, a sua organização pode ser obrigada a seguir alguma outra, como por exemplo, o NIST do governo norte americano. O importante é que fique explícito para todos qual a arquitetura que a organização segue.

4. Avalie a Arquitetura de Segurança e os Controles dos Direcionadores

Tomando por base o conjunto de controles (amplos ou específicos) definidos nos direcionadores obrigatórios, verifique se a Arquitetura de Segurança da Informação adotada, atende ou possibilita atender estes controles. Como dissemos anteriormente, talvez a arquitetura não defina especificamente o controle necessário, mas se esta arquitetura contempla o assunto do controle, podemos assumir que esta arquitetura é adequada.

Nesta etapa, caso a arquitetura adotada considere os controles exigidos pelos direcionadores corporativos, podemos afirmar que a Gestão de Compliance da Informação poderá acontecer de maneira adequada seguindo esta arquitetura.

Segue abaixo um exemplo onde verificamos se a legislação brasileira de tratamento de informação e alguns normativos do Banco Central do Brasil, são contemplados pela Arquitetura de Segurança da Informação baseada na Norma ISO/IEC 27002:2013. Neste exemplo fica facilmente visível que esta arquitetura atende os controles considerados e também indica que esta arquitetura contempla duas dimensões (Ambiente Físico e Modelo Operativo S.I.) que não são exigidos na legislação nem nos normativos considerados do BC.

Legislação e BC (alguns) x Arquitetura Segurança Informação ISO 27002

	DIMENSÕES DE SEGURANÇA DA INFORMAÇÃO														
NORMATIVOS E LEGISLAÇÃO ⬇	Política de S.I.	Acesso Informação	Classificação Informação	Proteção Técnica	Flexibilidade Operacional	Desenvolv. Aplicativos	Continuidade Negócio	Cópias de Segurança	Gestão de Riscos S.I.	Gestão Incidentes	Treinamento em S.I.	Ambiente Físico	Modelo Operativo S.I.	Atend. Auditoria	Processo Corporativo S.I.
Resolução 3694 - Prevenção de Riscos Serviços IF		X	X			X		X	X						
Resolução BC 4282 - Supervisão Arranjos Pagamento - SPB	X														
Circular BC 3681 - Gerenciamento de Riscos I. Pagamento		X	X	X	X	X			X						X
Circular BC 3682 - Arranjos Pagamento - SPB							X							X	X
Circular BC 3683 - Funcionando Instituições Financeira							X	X	X						X
Resolução BC 3380 - Gerenciamento Risco Operacional									X						
Resolução BC 2554 - Implantação Controles Internos		X				X	X		X		X			X	
Lei Compl. 105/2001 - Sigilo Instituições Financeiras			X				X	X						X	X
Lei 7492/1986 - Crimes contra Sistema Financeiro		X													
Lei 12737 - Delitos Informáticos															X
Lei 12965 de 2014 - Marco Civil da Internet		X	X			X		X							
Lei 12683 de 2012 - Crimes de Lavagem de Dinheiro		X	X												X
Lei 7963 de 2013 - Plano Nacional Consumo Cidadania		X	X			X		X							X
Lei 7962 de 2013 - Contratação no Comércio Eletrônico															X
Ante Projeto - Tratamento de Dados Pessoais	X	X	X		X	X				X					X

5. Avalie a efetividade do funcionamento dos controles da Arquitetura de Segurança

Esta é a etapa da verdade! Avalie a maturidade do atendimento dos controles. É neste ponto que concretamente saberemos se a organização está adequadamente em conformidade com os direcionadores. Podemos afirmar que nesta etapa a Gestão de Compliance da Informação acontece. Ou não.

Uma sugestão: se você vai realizar a primeira avaliação, considere inicialmente os macrocontroles. Outra opção para organizações muito grandes é considerar um determinado escopo. Temos que ter o cuidado com o tamanho do projeto de avaliação de maturidade dos controles.

6. Divulgue o Nível de Compliance e planeje as ações de melhoria

O nível atual de Compliance da Informação da organização deve ser divulgado internamente para o Corpo Diretivo. Porém, não se encerra com esta atividade. É necessário, considerando o não atendimento dos controles de Compliance de Informação, a elaboração de um planejamento de ações para que a organização atinja o seu patamar adequado de Compliance da Informação.

7. Estamos falando de Gestão de Compliance

Muitas vezes o Compliance é tomado como um fato. É necessário encarar uma Gestão de Compliance, e no nosso caso, uma Gestão de Compliance da Informação. Sendo assim é necessário a realização das etapas anteriores em um ciclo de gestão, em um ciclo de melhoria, tipo PDCA.

A Gestão da Segurança da Informação e a Gestão de Compliance da Informação se encaixam como peças de um quebra cabeça cujo objetivo é o atendimento dos objetivos corporativos. O mais importante é este conjunto de peças se encaixar adequadamente e trabalhar junto para o atendimento aos objetivos corporativos.

Normalmente se destaca o Compliance pelo seu valor legal, mas, Compliance é mais do que legislação: é o atendimento ao que a organização quer considerar como direcionador.

E Segurança da Informação é mais do que Compliance. Sendo assim, a junção de Segurança da Informação e Compliance protege a informação e permite a sustentabilidade, continuidade e atendimento aos objetivos da organização.

Fonte: LEC, em 21.11.2016.