IMPLEMENTAÇÃO DE UM SISTEMA UNIFICADO DE GESTÃO DA SEGURANÇA DA INFORMAÇÃO EM DATA CENTERS DE DIVERSOS PAÍSES [1]

Fabrício Avancini

Resumo: A proposta deste artigo é demonstrar o planejamento e o levantamento dos principais pontos de atenção com relação à implementação de um Sistema de Gestão da Segurança da Informação (SGSI), de acordo com a ABNT NBR ISO/IEC 27001:2013 em uma empresa que presta serviços de Data Center na Argentina, Brasil, Chile, Colômbia, Equador e Peru. Através de pesquisa e aplicação serão avaliadas questões legais, culturais e outras que podem influenciar na correta implementação do SGSI, bem como na elaboração e aplicação de políticas, procedimentos, registros e verificações pertinentes à Segurança da Informação.

Palavras-chave: Segurança da Informação. SGSI. ABNT NBR ISO/IEC 27001:2013.

1 INTRODUÇÃO

A implementação de um Sistema de Gestão da Segurança da Informação, de acordo com a norma internacional ABNT NBR ISO/IEC 27001:2013, é bastante complexa ao considerar os diversos processos e ativos de uma empresa que presta serviços de Data Center. O desafio encontrado é determinar como deve ser a abordagem para obter sucesso na implementação, certificação e manutenção de um SGSI (Sistema de Gestão da Segurança da Informação) considerando filiais em países diferentes, com culturas, problemas e leis específicas e distintos entre si.

Conforme descrito na ABNT NBR ISO/IEC 27002 (2013, P. vi), a segurança da informação é obtida pela implementação de um conjunto adequado de controles, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de software e hardware. Esses controles precisam ser estabelecidos, implementados, monitorados, revisados e melhorados, quando necessário, para assegurar que a segurança

[1] Artigo apresentado como Trabalho de Conclusão do Curso de Especialização em Segurança da Informação, da Universidade do Sul de Santa Catarina, como requisito parcial para a obtenção do título de Especialista em Segurança da Informação.

e os objetivos específicos do negócio da organização são atendidos. Um SGSI como o especificado na norma ISO / IEC 27001 adota uma visão holística e coordenada dos riscos de segurança da informação da organização a fim de implementar um conjunto abrangente de controles de segurança da informação sob a estrutura geral de um sistema de gestão coerente.

Nesse contexto busca-se determinar qual seria a melhor abordagem para adequar o Sistema de Gestão e os controles aplicados às diferenças culturais e legais que existem entre os países envolvidos na implementação, que são Argentina, Brasil, Chile, Colômbia, Equador e Perú.

2 SISTEMA DE GESTÃO DA SEGURANÇA DA INFORMAÇÃO

2.1 PLANEJAMENTO DO SGSI

Um Sistema de Gestão da Segurança da Informação está baseado em três pilares: confidencialidade, integridade e disponibilidade que são assim definidos por SÊMOLA (2014, p.43):

- Confidencialidade: toda informação deve ser protegida de acordo com o grau de sigilo de seu conteúdo, limitando o seu acesso somente a pessoas autorizadas;
- Integridade: toda informação deve ser mantida na condição em que foi disponibilizada pelo seu proprietário, protegendo-a contra alterações indevidas, intencionais ou acidentais; e
- Disponibilidade: toda informação gerada deve estar disponível para os seus usuários no momento em que ela for solicitada para qualquer fim.

Para iniciar a implementação de um SGSI deve-se definir um escopo, que delimita quais processos e serviços serão cobertos pelo Sistema de Gestão. Em seguida é preciso identificar todos os ativos que fazem parte desse alcance, bem como seus proprietários, a fim de utilizá-los como entradas para uma Análise de Riscos e a devida aplicação de controles, a fim de mitigar os riscos identificados.

Em um escopo que abrange diversos países, a aplicação dos controles selecionados pode sofrer alterações devido a fatores legais, geográficos, econômicos, entre outros. Um bom exemplo disso é a aplicação do controle A.7.1.1 – Seleção, definido na ABNT NBR ISO/IEC 27001 – Anexo A (2013, p.13). Esse controle define que verificações do histórico devem ser realizadas para todos os candidatos a emprego, de acordo com a ética, regulamentações e leis relevantes, e deve ser proporcional aos requisitos do negócio, aos riscos percebidos e à classificação das informações a serem acessadas. No Brasil, a legislação vigente impede que seja feita qualquer verificação no histórico do candidato como forma de seleção. Em outros países, como Argentina, Colômbia e Peru, por exemplo, essa verificação é permitida.

Outro controle de grande importância para um SGSI pode ser encontrado no item A.7.2.2 – Conscientização, educação e treinamento em segurança da informação, definido na ABNT NBR ISO/IEC 27001 – Anexo A (2013, p.14). A correta aplicação desse controle é fundamental, uma vez que visa mitigar um dos maiores riscos para um SGSI: o fator humano, como foi mencionado por Mitnick e Simon (2003, p.3): Uma empresa pode ter adquirido as melhores tecnologias de segurança que o dinheiro pode comprar, pode ter treinado seu pessoal tão bem que eles trancam todos os segredos antes de ir embora e pode ter contratado guardas para o prédio na melhor empresa de segurança que existe. Mesmo assim essa empresa ainda estará vulnerável. Os indivíduos podem seguir cada uma das melhores práticas de segurança recomendadas pelos especialistas, podem instalar cada produto de segurança recomendado e vigiar muito bem a configuração adequada do sistema e a aplicação das correções de segurança. Esses indivíduos ainda estarão completamente vulneráveis.

2.2 ESCOPO DO SGSI

O escopo definido para o SGSI da empresa foi: “Prestação de serviços oferecidos nos Data Centers de Argentina, Brasil, Chile, Colômbia, Equador e Peru”.

3 IMPLEMENTAÇÃO DO SGSI

A implementação do Sistema de Gestão da Segurança da Informação seguiu o plano apresentado a seguir, que descreve as etapas principais que devem ser seguidas a fim de implementar um SGSI dentro do escopo apresentado anteriormente.

3.1 Plano de Implementação

3.1.1 Planejamento do SGSI:

- Definição de líder de projeto
- Definição de alcance do SGSI
- Definição de equipo de projeto
- Direção regional - Minuta de reunião: Determinação do início do projeto, recursos e escopo
- Direção local - Minuta de reunião: Designação de papéis, comunicação
- Levantamento de requisitos legais, locais e regionais
- Kick-off interno
- Gap analysis

3.1.2 Estabelecimento do processo de avaliação de riscos

- Revisão do processo de avaliação de risco para alinhá-lo com os novos países
- Elaboração de material de capacitação
- Avaliação de riscos
    - Treinamento no processo de avaliação de risco
    - Identificação de ativos
    - Identificação de riscos
    - Análise e avaliação de riscos
- Tratamento de riscos
    - Treinamento sobre o processo de tratamento de riscos
    - Seleção de opções para tratamento de riscos
    - Seleção de objetivos e controles para tratamento de riscos
    - Elaboração de SoA - Declaração de aplicabilidade
    - Formulação do plano de tratamento de riscos e aprovação pelos proprietários de riscos
    - Aceitação de riscos residuais pelos proprietários dos riscos, após o tratamento dos mesmos
    - Determinação dos objetivos de segurança da informação

- Implementação do plano de tratamento de riscos
    - Sensibilização sobre políticas, contribuição para a eficácia do SGSI, benefícios da melhoria do desempenho da segurança da informação e implicações do não cumprimento
    - Implementação do plano de tratamento de riscos

3.1.3 Monitoramento, medição, análise e avaliação

- Determinar o que monitorar e medir, métodos e responsáveis
- Determinar análise e avaliação

3.1.4 Implementação do SGSI

- Kick-off com Áreas envolvidas
- Determinação das comunicações internas e externas relevantes para o SGSI
- Informação documentada a ser elaborada:
    - Escopo do SGSI: Parte do Manual do Sistema de Gestão
    - Políticas:
        - Política de controle de acesso físico
        - Política de negócios não estândar
        - Política de Controle de Acesso
        - Política de monitoramento
        - Política de acceso remoto a las redes internas
        - Política de Gestão e Controle de Mídias
        - Política Criptográfica
        - Política de Generación y Tratamiento de Logs
        - Política de Antivírus
        - Política de Administración de Dispositivos de Red
        - Política de Utilização de Tecnologias Críticas
        - Política de Segurança da Informação
        - Política de Patches de Segurança
    - Procedimentos:
        - A lista de procedimentos e outros documentos pode ser encontrada no item 3.2

- Objetivos
- SoA (Declaração de Aplicabilidade)
- Evidências de competência do pessoal
- Evidências de que os processos são realizados de acordo com o planejado
- Resultados da avaliação de riscos
- Resultado do tratamento dos riscos
- Resultados de monitoramento e medição
- Programa de auditorias e resultados de auditorias ISO 27001
- Resultados de Análises Críticas pela Direção
- Evidências e Resultados de tratamento de Ações Corretivas.

3.1.5 Realização da Auditoria Interna

3.1.6 Tratamento de ocorrências da Auditoria Interna

3.1.7 Realização da Auditoria Externa

3.2 LISTA DE DOCUMENTOS CRIADOS PARA A IMPLEMENTAÇÃO DO SGSI

A tabela a seguir apresenta os procedimentos e outros documentos criados para atender os principais itens da ISO 27001.

Itens da norma ISO 27001	Documentos Gerados
4 Contexto da organização	Parte do Manual do SGSI
4.1 Entendendo a organização e seu contexto	Contexto e Conhecimento Organizacional
4.2 Entendendo as necessidades das partes interessadas	Parte do Manual do SGSI
4.3 Determinando o escopo do SGSI	Parte do Manual do SGSI
4.4 Sistema de Gestão da Segurança da Informação	Parte do Manual do SGSI
5 Liderança	Parte do Manual do SGSI
5.2 Políticas	Política Geral do Sistema Integrado de Gestão
5.3 Papéis organizacionais, responsabilidade e autoridades	Registro de nomeações
6 Planejamento	Procedimento para a Análise Crítica pela Direção Registro de nomeações
6.1 Ações para identificar riscos e oportunidades	Procedimento para a Análise Crítica pela Direção Procedimento para a gestão de detecções
6.2 Objetivos de segurança da informação e planejamento para obtê-los	Procedimento para a Análise Crítica pela Direção Registro de nomeações

7 Apoio	Parte do Manual do SGSI
7.1 Recursos	Procedimento para a Análise Crítica pela Direção
7.2 Competência	Procedimento para a gestão de perssoas Procedimento para a gestão da capacitação Controle de participação em capacitações Registro de certificações colaboradores DC Registro de capacitações colaboradores DC Registro de nomeações
7.3 Conscientização	Procedimento para a gestão da capacitação Processo Disciplinar Controle de participação em capacitações Registro de certificações colaboradores DC Registro de capacitações colaboradores DC Registro de nomeações
7.4 Comunicação	Plano de Comunicação
7.5 Informação documentada	Procedimento para a gestão de documentos e registros Registro de documentos externos Procedimento para a gestão de detecções
7.5.1 Geral	Parte do Manual do SGSI
7.5.2 Criando e atualizando	Procedimento para a gestão de documentos e registros Registro de documentos internos Registro de documentos externos Registro de cópias controladas
7.5.3 Controle de informação documentada	Procedimento para a gestão de documentos e registros
8 Operação	Procedimento para a Gestão de Riscos
8.1 Planejamento e controle operacional	Procedimento de Instalação para o Delivery de serviços de Data Center Procedimento de Operação de serviços de Data Center
9 Avaliação de desempenho	Parte do Manual do SGSI
9.1 Monitoramento, medição, análise e avaliação	Parte do Manual do SGSI
9.1.1 Geral	Procedimento para a gestão de auditorias Procedimento para a gestão de incidentes Procedimento para a Análise Crítica pela Direção Procedimento para a gestão de detecções
9.1.2 Satisfação do Cliente	Procedimento para a avaliação da satisfação dos clientes
9.1.3 Análise e Avaliação	Procedimento para a Análise Crítica pela Direção
9.2 Auditoria interna	Procedimento para a gestão de auditorias
9.3 Análise crítica pela Direção	Procedimento para a Análise Crítica pela Direção

10 Melhoria	Parte do Manual do SGSI
10.1 Não-conformidade e medidas corretivas	Procedimento para a gestão de detecções
10.2 Melhoria contínua	Parte do Manual do SGSI

3.3 PARTICULARIDADES REGIONAIS NA IMPLEMENTAÇÃO DO SGSI

3.3.1 Leis de Proteção de Dados Pessoais – Controle A.18.1

Alguns países da América Latina já possuem leis específicas com respeito à proteção de dados pessoais, tais como a Lei nº 25.326 (ARGENTINA, 2000), a Lei nº 19.628 (CHILE, 2012), a Lei nº 1.581 (COLÔMBIA, 2012) e a Lei nº 29.733 (PERÚ, 2011). No Brasil, neste momento, existe o Projeto de Lei da Câmara nº 53 (BRASIL, 2018) que trata desse tema e deverá entrar em vigor em breve.

Essas leis têm um conjunto de requisitos bastante similar e definem diretrizes para a coleta, armazenamento, tratamento e distribuição de dados pessoais, tais como nome, correio eletrônico, número de documentos, dados biométricos, informações sobre saúde, entre outros.

3.3.2 Verificação de histórico do funcionário – Controle A.7.1.1

A prática da exigência de atestado de antecedentes e a investigação do passado profissional dos funcionários é uma questão controversa e possui particularidades em cada país. No Brasil, por exemplo, é uma prática que caiu em desuso nos últimos anos, principalmente por alegações de discriminação.

3.3.3 Acesso Físico – Controle A.11.1.1

A revista pessoal, em bolsas e mochilas, é uma prática que não é permitida em todos os países. Na Argentina e Peru, por exemplo, é permitida, enquanto no Brasil possui restrições.

3.3.4 Idioma

Os documentos listados no item 2.4 e registros gerados pelo SGSI devem ser gerados e controlados nos idiomas Português e Espanhol.

3.4 CONCLUSÕES

Para a correta implementação de um SGSI em diversos países, foi necessário um grande cuidado no levantamento e na aplicação da legislação local, que pode ser diferente em cada país. Com relação à revista pessoal, monitoramento de imagens e correios eletrônicos, por exemplo, foi necessário definir qual a legislação mais restritiva e aplica-la a toda a região, uma vez que a comunicação, imagens e outros podem circular entre os países com leis diferentes.

No caso das Leis de proteção de dados pessoais, a melhor solução é aplicar a legislação mais restritiva e abrangente a todos os países, desde que não seja contrária a nenhuma outra lei local. A proteção dos dados pessoais não deverá, por exemplo, atrapalhar uma investigação policial ou acobertar algum ato ilícito praticado em virtude da proteção de dados.

As diferenças culturais devem ser observadas no momento de definir políticas, bem como nas capacitações, que podem ser recebidas de distintas maneiras em cada local. Ainda que uma determinada prática não seja ilegal em algum país, pode ser considerada antiética em virtude de algum costume ou cultura local.

Um dos desafios, talvez o maior, na implementação de um SGSI transnacional é a necessidade de uma atenção especial ao relacionamento profissional transcultural, uma vez que a maior parte da comunicação e do relacionamento será realizado majoritariamente de forma virtual, através de correios eletrônicos, vídeo conferências, telefonemas. Ademais da cultura, a diferença no idioma é uma questão importante a ser considerada, uma vez que pode prejudicar a comunicação e, consequentemente, a correta aplicação de Políticas e Procedimentos.

A realização de auditorias, principalmente internas, deve ser alvo de um cuidadoso planejamento, já que envolve diversos deslocamentos e alocação de pessoal. Por experiência, o uso de diversos auditores, locais, é mais recomendada do que alocar uma pessoa para realizar auditorias em diversos países diferentes, pois evita o choque cultural e propicia uma avaliação mais apurada de questões locais, como legislação, costumes e outros.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27001: TECNOLOGIA DA INFORMAÇÃO -TÉCNICAS DE SEGURANÇA - SISTEMAS DE GESTÃO DA SEGURANÇA DA INFORMAÇÃO - REQUISITOS**. 2 ED. RIO DE JANEIRO: ABNT, 2013. 30 P.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27002: TECNOLOGIA DA INFORMAÇÃO - TÉCNICAS DE SEGURANÇA -**

CÓDIGO DE PRÁTICAS PARA CONTROLES DE SEGURANÇA DA INFORMAÇÃO. 2 ED. RIO DE JANEIRO: ABNT, 2013. 90 P.

SÊMOLA, Marcos. **Gestão da Segurança da Informação. Uma visão executiva**. 2. Ed. El-sevier Brasil, 2014.

MITNICK, Kevin D.; SIMON, William L.. **MITNICK - A arte de enganar**. São Paulo: Pearson Education, 2003. 284 p.

ARGENTINA. Lei nº 25.326, de 04 de novembro de 2000. **Proteccion de Los Datos Personales**. Buenos Aires, Disponível em: <http://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/norma.htm>. Acesso em: 22 jul. 2018.

BRASIL. Projeto de Lei da Câmara nº 53, de 2018. **Proteção de Dados Pessoais**. Brasília, Disponível em: <https://legis.senado.leg.br/sdleg-getter/documento?dm=7738646&disposition=inline>. Acesso em: 22 jul. 2018.

CHILE. Lei nº 19.628, de 17 de fevereiro de 2012. **Protección de Datos de Caracter Personal**. Santiago, Disponível em: <https://www.leychile.cl/Navegar?idNorma=141599&buscar=19628>. Acesso em: 22 jul. 2018.

COLÔMBIA. Lei nº 1.581, de 17 de outubro de 2012. **Proteccion de Los Datos Personales**. Bogotá, Disponível em: <https://habeasdatacolombia.uniandes.edu.co/wp-content/uploads/LEY-1581-DEL-17-DE-OCTUBRE-DE-2012.pdf>. Acesso em: 22 jul. 2018.

PERÚ. Lei nº 29.733, de 03 de julho de 2011. **Ley de protección de datos personales**. Lima, Disponível em: <https://www.minjus.gob.pe/wp-content/uploads/2013/04/LEY-29733.pdf>. Acesso em: 22 jul. 2018.