ASEGI

Associação Brasileira de Profissionais e Empresas de Segurança da Informação e Defesa Cibernética

Norma Brasileira de Gestão de Segurança da Informação (NBSI) - 01/2017

Esta norma foi escrita pelo comitê formado pelos seguintes membros:

Alexandre Knoploch
Bruno Macena
Ivan Lindenberg Junior
Marcus Fábio Fontenelle do Carmo
Paulo Maurício Espanha

Sede:
Avenida Franklin Roosevelt, 23 – Centro
Rio de Janeiro – RJ: CEP: 20021-120
Tel: +55 21 2533-5284
asegi@asegibrasil.com.br
www.asegibrasil.com.br

ASEGI – BRASIL
v.01/2017
18/07/2017

Prefácio

A Associação Brasileira de Profissionais e Empresas de Segurança da Informação e Defesa Cibernética (ASEGI) é constituída por membros da Comunidade Brasileira de Segurança da Informação e Defesa Cibernética que, através desta associação, criaram uma norma genuinamente brasileira, tendo como intuito a orientação e a criação de uma normativa que institui em nosso país empresas que observem o caráter protetivo da informação de forma mais consistente e processual, criando um cenário de estabilidade confidencial e segurança para suas ações e seus clientes.

A NBSI pode ser perfeitamente trabalhada em consonância com outras normativas de segurança da informação, visando sempre a melhoria contínua dos processos de segurança da informação.

Esta norma foi desenvolvida a partir das peculiaridades brasileiras no cumprimento de boas práticas de segurança da informação, além de ser de simples adoção para qualquer organização.

A implantação da NBSI deverá respeitar o direito à privacidade definido no art. 5º, inciso X, da Constituição da República Federativa do Brasil de 1988.

Acreditamos que esta norma irá melhorar o dia a dia das empresas diante dos processos de segurança e trazer melhor respaldo técnico e legal para seus gestores executivos e operacionais.

Sumário

1. Introdução

1.1. A ASEGI Brasil é a entidade mantenedora exclusiva desta norma e suas versões.

1.2. Organizações que aderirem a esta norma poderão se candidatar à certificação da NBSI, emitida pela ASEGI, para o escopo que especificarem.

1.3. As diretrizes estabelecidas por esta norma proporcionarão a implementação de um sistema de segurança da informação mínimo nas organizações.

1.4. O solicitante do certificado ASEGI - NBSI deverá ser auditado por uma empresa credenciada pela ASEGI e obter a conformidade de 70% (setenta por cento) dentro de 16 (dezesseis) questões que poderão ser escolhidas a critério do auditor, observando esta norma.

2. Geral

2.1. Esta norma especifica os requisitos que visam mitigar os riscos em segurança da informação, assim como melhorar de forma contínua os processos de gestão desse escopo.

2.2. A segurança da informação existe para proteger a informação e o negócio. Portanto, é necessário um alinhamento mínimo com a governança corporativa da organização.

2.3. O sistema de segurança da informação da organização será composto pelos requisitos propostos por esta norma e demais ações implementadas pela organização.

2.4. É recomendável que o sistema de segurança da informação contemple ações para proteger a informação em qualquer meio em que ela esteja contida.

2.5. É recomendável que as organizações estabeleçam metas de segurança da informação e indicadores de controle dessas metas.

2.6. É recomendável que o cumprimento dos requisitos não ocorra de forma isolada, devendo haver uma integração.

3. Aplicação

Esta norma pode ser aplicada a todas as organizações, independentemente de tipo, tamanho e natureza.

4. Compatibilidade

Empresas já detentoras da certificação ISO 27001 ficam dispensadas de auditoria, podendo apenas apresentar a certificação em pleno gozo de validade.

5. Política de Segurança

5.1. A criação da política de segurança deve respeitar a característica do negócio, evitando o desuso da política e a resistência da organização.

5.2. É recomendada a criação de políticas menores de organização e que evitem a exposição de informações.

5.3. É recomendado, dependendo do contexto da organização, a elaboração de um documento de política de segurança geral com desmembramento de documentos específicos para áreas técnicas.

6. Segurança da Informação e a Organização

6.1. Requisitos Gerais

6.1.1. A organização deve estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar diante das necessidades a operação de segurança da informação.

6.1.2. Para gestão operacional, não é necessária a criação de uma estrutura organizacional, porém é necessário que seja realizada por pessoas devidamente designadas para essa função, com conhecimento sobre riscos, ameaças, tecnologia e processos que são inerentes ao conceito de segurança da informação.

6.2. A definição de papéis trata-se da concepção organizacional de atribuir responsáveis por cada ação dentro da organização, tornando explícito e acessível aos usuários o papel de cada um na gestão operacional.

6.3. Para o funcionamento pleno de processos de segurança da informação e todo sistema definido para tal, é necessária a participação dos gestores de diversos setores, o que possibilitará uma visão completa de toda a organização no que tange às normas e processos implementados ou em fase de implementação.

6.4. Criar programas de treinamento e normas de segurança é o caminho mais assertivo para a educação e conscientização dos colaboradores no processo de segurança da informação da organização.

6.5. Acordos de confidencialidade a informações acessadas trazem segurança jurídica e devem ser usados como forma de prevenção a vazamento de conteúdos sigilosos.

7. Escopo Selecionado

7.1. As organizações poderão selecionar escopo específico para implantação desta norma.

7.2. A seleção de um escopo específico não limitará o atendimento de alguns requisitos que deverão estar em toda a organização.

8. Gestão de Ativos

8.1. É requisito básico a legalidade de todos os ativos existentes na organização.

8.2. É necessária a criação de inventário dos ativos atualizados a fim de sempre saber onde existem informações e possibilidade de transmissão.

8.3. É necessário classificar as informações diante dos procedimentos que cada uma delas deve seguir, visando a garantia da integridade, disponibilidade e confidencialidade.

8.4. Deve-se levar em consideração também os dispositivos móveis e em nuvem, sendo importante garantir a autenticidade dos mesmos.

9. Gestão de Riscos de Segurança da Informação

9.1. É mandatório que a gestão de riscos de segurança da informação contemple a identificação dos riscos, o grau de ameaça e o plano de ação.

9.2. É mandatório que as organizações promovam ações para avaliar os principais riscos mapeados.

9.3. É mandatório que as organizações promovam ações para manter atualizado o mapeamento dos principais riscos de segurança da informação.

9.4. É mandatório que as organizações promovam ações para tratar os riscos mapeados.

9.5. É recomendável que as organizações, após o tratamento de riscos, tenham relação clara dos riscos aceitos.

10. Documentação, Comunicação e Conscientização

10.1. As organizações deverão manter documentação necessária que evidencie o cumprimento de todos os requisitos exigidos por esta norma.

10.2. É recomendável que as organizações promovam, através dos meios necessários, a comunicação e a divulgação da política de segurança da informação e demais documentos vinculados à segurança da informação, bem como os resultados obtidos.

10.3. É recomendável que as organizações promovam ações de capacitação e reciclagem visando a conscientização dos objetivos de segurança da informação.

11. Gestão de Acesso

11.1. É mandatório que as organizações tenham uma gestão de acesso que contemple o controle de acesso: físico, de ativos e de sistemas ou aplicações.

11.2. É mandatório que a gestão de acesso contemple uma revisão periódica dos direitos de acesso dos usuários.

11.3. É recomendável que a gestão de acesso contemple o acesso ao ambiente interno e externo da organização.

11.4. É mandatório restringir o acesso como usuário administrador das máquinas.

11.5. É mandatório usar senhas para acessos a ambientes de rede e sistemas.

11.6. É recomendável que todas as senhas possuam uma quantidade mínima de 8 (oito) caracteres, combinando três das quatro categorias a seguir:

- ✓ Letras maiúsculas do alfabeto (A – Z);
- ✓ Letras minúsculas do alfabeto (a – z);
- ✓ Números (0 – 9);
- ✓ Caracteres especiais (` ~ ! @ # $ % ^ & * ( ) _ - + = { } [ ] \ | : ; " ' < > , . ? /).

11.7. Recomenda-se o uso de duplo fator de autenticação em aplicações e na rede de computadores.

11.7.1.Torna-se mandatório o cumprimento deste item para corporações que armazenam dados de usuário privado e/ou sigiloso.

11.8. Recomenda-se a criação de política para uso de serviços de rede.

11.9. Recomenda-se a autenticação dos usuários para conexões externas.

11.10. Deve-se existir procedimento de *logon* no terminal.

11.11. Em caso de utilização de nuvem, deve-se oficializar qual tecnologia e fabricante a organização utilizará e informar aos usuários que utilizam esta tecnologia, evitando o uso de nuvens desconhecidas pela gestão de segurança.

11.12. Deve-se estender as regras de acesso para dispositivos móveis.

12. Ciclo de Vida das Aplicações e Manutenção

12.1. É recomendável que as organizações incluam regras de segurança da informação no ciclo de vida de suas aplicações.

12.2. É recomendável que as organizações realizem testes e homologações de suas aplicações antes da implementação, para minimizar riscos.

12.3. É recomendável que as aplicações tenham controles de segurança e criptografia.

12.4. É recomendável que as organizações implementem uma gestão de mudanças para o seu ambiente de TI.

12.5. Deve-se criar ambientes isolados de desenvolvimento e produção.

13. Gestão de Incidentes e Continuidade do Negócio

13.1. É recomendável que as organizações consigam gerenciar os incidentes de segurança da informação.

13.2. É recomendável que as organizações tenham procedimento de respostas a incidentes.

13.3. É recomendável que as organizações tenham um plano de continuidade do negócio.

13.4. É recomendável que o plano de continuidade do negócio seja testado e reavaliado a cada 6 (seis) meses.

13.5. Deve-se comunicar todos os eventos de segurança aos responsáveis identificados em uma Matriz de Responsabilidade a ser elaborada.

14. Melhoria Continuada

14.1. É recomendável que as organizações promovam ações de monitoramento e revisão das metas estabelecidas.

14.2. É recomendável que as organizações promovam auditorias para certificar o cumprimento dos requisitos de seu sistema de segurança da informação.

14.3. É recomendável que as organizações promovam periodicamente análise de falhas no sistema de segurança e de desvios nas metas.

14.4. É recomendável que as organizações, após a análise das falhas ou desvios, promovam ações para corrigi-las.

14.5. É recomendável que as organizações promovam periodicamente ações proativas para melhoria de seu sistema de segurança da informação.

15. Gestão de Operação

15.1. Cada item e procedimento mencionado na política de segurança deve ser documentado e armazenado em lugar seguro, criando um histórico documental e evidências de ações.

15.2. A criação de uma lista de checagem para introduzir um novo sistema é importante para evitar possíveis contaminações ou vulnerabilidades.

15.3. Deve-se controlar e ter ferramentas de bloqueio para softwares piratas.

15.4. Recomenda-se que sejam rastreados e armazenados os logs com as falhas detectadas.

15.4. Recomenda-se manter o registro das auditorias e de toda a movimentação de usuários e acessos.

Adesão à Norma Brasileira de Segurança da informação.

A organização que optar por aderir a esta norma deverá seguir as seguintes etapas:

I. Buscar adequação de sua organização conforme descrito nesta norma;
II. Contratar empresa auditora e creditadora homologada pela ASEGI;
III. Estar em conformidade e creditado pela auditoria;
IV. Pagar a taxa junto a ASEGI para homologação, certificado físico e selo digital.

- A validade da certificação é de um ano.