DIRETRIZES BÁSICAS DA POLITICA DE SEGURANÇA CIBERNÉTICA

SUMÁRIO

DIRETRIZES BÁSICAS DA POLITICA DE SEGURANÇA CIBERNÉTICA

1. INTRODUÇÃO

A Resolução CMN nº 4.658/18 determina que as instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil devem implementar e manter política de segurança cibernética formulada com base em princípios e diretrizes que busquem assegurar a confidencialidade, a integridade e a disponibilidade dos dados e dos sistemas de informação utilizados.

Essa política deve ser compatível com o porte, o perfil de risco e o modelo de negócio da instituição; a natureza das operações e a complexidade dos produtos, serviços, atividades e processos da instituição; e a sensibilidade dos dados e das informações sob responsabilidade da instituição.

2. SEGURANÇA CIBERNÉTICA

Segurança da Informação é o processo que tem como objetivo proteger a informação de diversos tipos de ameaças para garantir os negócios quanto à continuidade, a minimização dos danos e a maximização do retorno dos investimentos e das oportunidades, garantindo a guarda, integridade, recuperação, inviolabilidade e sigilo dos dados e informações eletrônicos que, de alguma forma, estejam armazenados ou transitem nos meios informatizados disponibilizados pela DESENBAHIA.

O processo de Segurança da Informação também contempla o armazenamento e tramitação de documentação física, buscando manter a integridade, inviolabilidade, sigilo e possibilidade de recuperação da informação neste meio.

2.1. Princípios

2.1.1. A segurança da informação é aqui caracterizada pela preservação de:

a) Confidencialidade: garantia de que a informação é acessível somente por pessoas autorizadas a terem acesso;

b) Integridade: salvaguarda que informação está exata e completa, assim como seus métodos de processamento; e

c) Disponibilidade: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

2.1.2. Adicionalmente, outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade, podem também estar envolvidas (ABNT NBR ISO/IEC 17799:2005).

2.1.3. A Política de Segurança de Informação exige a aplicação de controles para garantir que os objetivos de segurança específicos da Desenbahia sejam atendidos. Dentre os procedimentos e controles adotados, inclui-se os voltados para reduzir a vulnerabilidade da Agência a incidentes, abrangendo a **autenticação**, a **criptografia**, a **prevenção e a detecção de intrusão**, a **prevenção a vazamento de informações**, a **realização periódica de testes e varreduras para detecção de vulnerabilidades**, a **proteção contra softwares maliciosos**, o **estabelecimento de mecanismos de rastreabilidade**, os **controles de acesso e de segmentação da rede de computadores** e **manutenção de cópias de segurança dos dados e das informações**.

2.1.4. Os controles de segurança devem ser adotados também no desenvolvimento de sistemas de informação e na adoção de novas tecnologias empregadas nas atividades da Agência.

2.2. Responsabilidades

2.2.1. O CRS indicará as metodologias e processos específicos para a realização do processo de segurança da informação, aplicáveis por toda a DESENBAHIA, de forma que a segurança seja parte do planejamento da informação, observando:

a) o alinhamento das ações de tecnologia em segurança da informação com as diretrizes e estratégias gerais da DESENBAHIA;

b) análise crítica e monitoração de incidentes de segurança da informação na DESENBAHIA reportados ao CRS;

c) disseminação de informações sobre boas práticas a serem adotadas pelos Colaboradores para reforçar a cultura de Segurança da Informação na Desenbahia.

2.2.2. O funcionamento do processo de Segurança da Informação não pode ser assegurado pela existência de uma estrutura isolada dentro da Desenbahia. Para tanto, é necessário o envolvimento das Diretorias, Gestores de Processos e do CRS, cabendo a alta administração decidir e apoiar as estratégias de melhoria contínua dos procedimentos relacionadas com a segurança cibernética.

3. DIRETRIZES

3.1. Tratamento da Informação

3.1.1. Toda informação gerada internamente ou obtida no mercado deve ser usada exclusivamente para atender aos interesses da DESENBAHIA, podendo ainda ser fornecida a terceiros, respeitadas as restrições da classificação das informações bem como das imposições legais.

3.1.2. Os usuários responsáveis pela gestão, pela guarda e pela atualização ou utilização de dados e informações são denominados, respectivamente, gestor, custodiante e usuário, cabendo a todos o uso adequado das informações.

3.1.3. A divulgação interna e externa das informações da DESENBAHIA, realizada de modo formal ou informal, deve levar em consideração a classificação das informações, conforme definido pelos Gestores de cada área.

3.1.4. Nos contratos estabelecidos com os colaboradores devem constar cláusulas de sigilo e confidencialidade.

3.1.5. Os gestores dos processos serão responsáveis pelos critérios de geração das informações, pela garantia da exatidão e integridade das mesmas, bem como pela classificação.

3.1.6. Cada usuário deve ter senha única, pessoal e intransferível, que o qualifique como responsável por todas as atividades desenvolvidas através dela.

3.1.7. O acesso para atualização das informações deve ser determinado pelo Gestor do processo onde ela está inserida, considerando, entre outros aspectos, a classificação e a integridade das informações.

3.1.8. O acesso à consulta deve ser estabelecido de acordo com as definições da classificação das informações.

3.1.9. A instalação de qualquer *software*, mesmo no caso dos licenciados para a Desenbahia, ficará a cargo da GTI.

3.1.10. Os sistemas de informação deverão ter trilhas de auditorias definidas e monitoradas, a fim de manter a proteção adequada dos ativos da organização.

3.1.11. Os dirigentes e colaboradores da DESENBAHIA, a fim de ratificar demais questões de segurança da informação são automaticamente submetidos a termo de responsabilidade denominado CONDIÇÕES PARA USO DE RECURSOS DE TECNOLOGIA E DA SEGURANÇA DA INFORMAÇÃO NA DESENBAHIA, disponível no Gerenciador de Documentos da Desenbahia (GDD).

3.2. Revisão de usuários ativos dos sistemas

3.2.1. A GTI, através da USI, é responsável por efetuar a revisão anual dos usuários ativos dos sistemas da Desenbahia. Nesta revisão a USI, com a colaboração dos gestores de sistemas, deve buscar localizar possíveis inconsistências nos acessos aos diversos sistemas disponibilizados na rede.

3.2.2. Os procedimentos para a realização desta revisão estão detalhados em normativo específico.

3.3. Plano de Ação e de Resposta a Incidentes

3.3.1. O Plano de ação e de resposta a incidentes deve ser estabelecido, visando à implementação da política de segurança cibernética, abrangendo, dentre outros aspectos:

a) as ações a serem desenvolvidas pela Desenbahia para adequar suas estruturas organizacional e operacional aos princípios e às diretrizes da política de segurança cibernética;

b) as rotinas, os procedimentos, os controles e as tecnologias a serem utilizados na prevenção e na resposta a incidentes, em conformidade com as diretrizes da política de segurança cibernética; e

c) a área responsável pelo registro e controle dos efeitos de incidentes relevantes.

3.3.2. Anualmente será elaborado relatório sobre a implementação do plano de ação e de resposta a incidentes, com data-base de 31 de dezembro, devendo ser aprovado pelo CAD até 31 de março do ano seguinte ao da data-base, e abordar, no mínimo:

a) a efetividade da implementação das ações a serem desenvolvidas pela Desenbahia para adequar suas estruturas organizacional e operacional aos princípios e às diretrizes da política de segurança cibernética;

b) o resumo dos resultados obtidos na implementação das rotinas, dos procedimentos, dos controles e das tecnologias a serem utilizados na prevenção e na resposta a incidentes;

c) os incidentes relevantes relacionados com o ambiente cibernético ocorridos no período; e

d) os resultados dos testes de continuidade de negócios, considerando cenários de indisponibilidade ocasionada por incidentes.

3.3.3. A relevância dos incidentes é o resultado do produto urgência x impacto. A urgência dos incidentes é medida com base no tempo de indisponibilidade que o nível de serviço pode suportar até que tenha um impacto significativo no negócio. O impacto é mensurado em função do efeito em que os níveis de serviços afetados causam para o negócio.

3.3.4. Os cenários de incidentes a serem considerados nos testes de continuidade de negócios devem observar os seguintes parâmetros:

a) o tipo de incidente e a classificação da relevância.

b) a avaliação de impacto do incidente nos ativos que suportam os processos críticos de negócio e da probabilidade de ocorrência do evento.

3.3.5. A metodologia e procedimentos para classificação da relevância dos incidentes e definição dos cenários de incidentes serão temas de capítulos específicos deste manual.

4. CAPACITAÇÃO E DIVULGAÇÃO

4.1. Capacitação e Conscientização em Segurança Cibernética

4.1.1. Os Colaboradores (empregados, terceiros e estagiários) devem ser capacitados para a utilização dos recursos de informação e para a aplicação dos conceitos de segurança, de forma a garantir a confidencialidade, a integridade e a disponibilidade das informações da DESENBAHIA.

4.1.2. Os Colaboradores deverão ser avaliados periodicamente acerca do conhecimento em segurança da informação.

4.1.3. A Gerência de Marketing e Produtos (GMP), com o apoio da GTI, deverá promover as ações relativas à prestação de informações a clientes e usuários sobre precauções na utilização de produtos e serviços financeiros. Tais ações estarão no escopo da política de relacionamento com clientes.

4.1.4. Os funcionários da área de TI que atuam na gestão dos serviços a serem contratados devem ser devidamente capacitados de forma a possuírem as competências necessários para a adequada gestão dos serviços, inclusive para o adequado monitoramento dos serviços a serem prestados através da análise de informações e uso de recursos providos.

4.2. Divulgação da Política Cibernética

4.2.1. A Política de Segurança Cibernética deve ser amplamente divulgada a todos os funcionários da instituição e às empresas prestadoras de serviços a terceiros, mediante linguagem clara, acessível e em nível de detalhamento compatível com as funções desempenhadas e com a sensibilidade das informações, visando a conscientização de todos sobre a importância da segurança para o desempenho de suas atividades.

4.2.2. Deverá ser divulgado ao público em geral, através do Site institucional, resumo contendo as linhas gerais da política de segurança cibernética.

4.2.3. Sem prejuízo do dever de sigilo e da livre concorrência, a Desenbahia poderá compartilhar as informações sobre os incidentes relevantes com as instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil. Esse compartilhamento deve abranger

informações sobre incidentes relevantes recebidas de empresas prestadoras de serviços a terceiros. As informações compartilhadas devem estar disponíveis ao Banco Central do Brasil.

4.2.4. O MTI será revisado anualmente e aprovado pela DCO e Conselho de Administração.

5. MONITORAMENTO DA POLÍTICA CIBERNÉTICA

A política cibernética será acompanhada pela Gerência de *Compliance* e Riscos (GCR) e pela Auditoria Interna (AUD), com vistas a assegurar a implementação e a efetividade da política, do plano de ação e de resposta a incidentes e dos requisitos para contratação de serviços de processamento e armazenamento de dados e de computação em nuvem, incluindo:

a) a definição de processos, testes e trilhas de auditoria;

b) a definição de métricas e indicadores adequados; e

c) a identificação e a correção de eventuais deficiências.