POLÍTICA
DE
SEGURANÇA CIBERNÉTICA

Atualizada em 05/2019

ÍNDICE

1. OBJETIVO

A Política de Segurança Cibernética (PSC) visa prover a metodologia necessária para prever os procedimentos e os controles adotados pelo Grupo Modal, prevenir e reduzir os riscos na resposta a incidentes relacionados ao ambiente cibernético, reforçar a conscientização do processo alinhado com as diretrizes institucionais, incluindo contratação de serviços de processamento e armazenamento de dados e de computação em nuvem para garantir a segurança das operações.

2. VIGÊNCIA, REVOGAÇÃO E CICLO DE REVISÃO

Esta política entra em vigor na data de sua publicação e permanecerá vigente, podendo ser revisada no caso de alteração na legislação ou se houver alguma alteração das práticas de negócios do Grupo Modal.

3. DIRETRIZES

As diretrizes de Segurança Cibernética do Grupo Modal têm os seguintes objetivos principais:

I. Estar em conformidade com a Resolução CMN, nº 4.658/2018 que dispõe sobre a política de segurança cibernética;

II. Assegurar que os procedimentos contenham no mínimo a descrição dos controles referentes à segurança;

III. Comunicar de forma tempestiva o Banco Central do Brasil das ocorrências de incidentes relevantes e das interrupções dos serviços relevantes, que configurem uma situação de crise pelo Grupo Modal, bem como das providências para o reinício das atividades;

IV. Definir procedimentos e controles voltados à prevenção e ao tratamento dos incidentes a serem adotados por empresas prestadoras de serviços a terceiros que manuseiem dados ou informações sensíveis, ou que sejam relevantes para a condução das atividades operacionais da instituição;

V. Definir procedimentos e controles voltados ao descarte e manutenção segura de dados e equipamentos;

VI. Definir os parâmetros de classificar os dados e as informações quanto à relevância;

VII. Monitorar serviços contratados;

VIII. Adotar práticas de governança corporativa e de gestão proporcionais à relevância do serviço a ser contratado e aos riscos a que estejam expostas;

4. REGRAS E CONTROLES

Os controles lógicos de sistema relevantes devem possuir gerenciamento na autenticação, validação segura de qualquer entrada de dados e manutenção de acordo com a metodologia interna, realização de testes visando identificação de vulnerabilidades e implementar controles contra softwares maliciosos, acesso controlado e monitorado a ambientes de produção, testes de penetração, controle de patches bem como manter as cópias de segurança de dados e das informações atualizadas.

Os acessos e a sua revisão devem ser regidos de acordo com a Norma de Controle de Acessos e suas segregações de funções, distribuição e controle de acessos físicos e/ou lógicos que possam conter informações das empresas do Grupo MODAL bem como possuir controles para proteger as informações utilizando as melhores práticas do mercado.

A avaliação das práticas de segurança deve ser parte do processo no desenvolvimento de sistemas relevantes tornando o processo de concepção dos sistemas construídos dentro do Modal mais confiável, e com controle de auditoria, estável e protegido contra ameaças atendendo os requisitos e metodologia interna assegurando que as informações processadas sejam protegidas.

Devem ser estabelecidos e continuamente aprimorados os controles de segurança cibernética afim de certificar que as informações sejam monitoradas e / ou os recursos de tecnologia sejam inspecionados nas dependências de fornecedores relevantes e que atendam o mínimo dos requisitos referentes a segurança cibernética tais como, a localização de onde os dados estão hospedados, continuidade, medidas de segurança para transferir e armazenar os dados, manutenção e proteção das informações de clientes na segregação de dados e dos controles de acesso físicos e lógicos e que os dados transferidos estejam íntegros e disponíveis na transferência de dados, bem como dados excluídos totalmente, quando solicitado.

O descarte de informações e ativos deve ser realizado de forma segura, com a utilização de equipamentos apropriados como fragmentadoras de acordo com as boas práticas internas garantindo assim confidencialidade dos dados.

5. CLASSIFICAÇÃO DA INFORMAÇÃO

Assegurar que as informações sejam classificação estejam elas armazenadas e ou em processamento, alinhado com as diretrizes institucionais e deve ser preservada e guardada em conformidade com as políticas, normas e procedimentos internos de acordo com a Norma de Classificação da Informação. O Modal, seus colaboradores e seus prestadores de serviço tem a missão de estar em conformidade com as leis sancionadas a fim de proteger as informações de seus clientes.

As informações sensíveis devem ser tratadas e armazenadas de forma segura e integra, bem como com os métodos de criptografia adequados e a proteção contra o vazamento de informações.

6. RESPOSTA A INCIDENTES

A resolução de incidentes cibernéticos consiste na definição dos critérios e procedimentos para mitigar riscos relacionados à segurança garantindo a detecção, classificação, registro, análise, tratamento e monitoração, onde são registradas todas as fases contendo inclusive analise da causa e impacto. A resposta de incidentes deve ser administrada de acordo com os requisitos específicos adotados e estabelecer critérios de avaliação e relevância de um incidente.

A tratativa de incidentes de segurança será realizada prioritariamente pela equipe do SOC, sendo esta a única proprietária do processo de tratamento, porém, durante o ciclo de vida do incidente, pode haver acionamento de equipes necessariamente envolvidas no processo, bem como acionamento de Fornecedores e Parceiros de acordo com sua necessidade para apoiar no tratamento de incidentes.

7. USO ACEITÁVEL

Os ativos corporativos devem ser geridos de acordo com os requisitos especificados na Norma de Uso Aceitáveis, bem como estabelecer regras para utilização, proteção das informações e garantir que todos os usuários usem os recursos de computação da empresa de maneira eficaz, eficiente, ética e lícita do Grupo Modal.

8. GESTÃO DE VULNERABILIDADES

A área de Segurança da Informação deve identificar, estabelecer, avaliar, classificar, solucionar, reduzir e documentar as vulnerabilidades relevantes nos sistemas interno e expostos na Internet continuamente, bem como monitorar as configurações básicas de segurança afim de verificar aplicabilidade adequada conforme procedimento interno.

9. CULTURA CIBERNÉTICA

O plano de conscientização de segurança cibernética abrange campanhas, termos de ciência e treinamentos periódicos para disseminar conhecimento para os colaboradores do Grupo Modal de modo que todos tenham um nível adequado de conhecimento e responsabilidade em proteger os ativos de informações. Este plano estabelece maneiras para zelar, minimizar e mitigar danos de segurança cibernética.

10. CONTINUIDADE DE NEGÓCIOS

O plano de continuidade de negócio deve estabelecer, implementar e manter procedimentos documentados para gerenciar interrupções e continuar suas atividades com base em objetivos de recuperação identificados em um tempo mínimo aceitável dentro do prazo acordado. Garantir que os procedimentos sejam testados com resultados satisfatórios para atendimento do negócio.

Fornecedores devem atender os requisitos de continuidade de negócios contemplando os testes em caso de interrupção de serviços críticos prestados ao Grupo Modal de processamento e armazenamento de dados e de computação em nuvem e o reestabelecimento da operação normal da Instituição.