Política de Segurança Cibernética – Resolução 4.658/CMN

1. Objetivo

A CONEXION tem por objetivo estabelecer diretrizes e responsabilidades para o gerenciamento da segurança da informação cibernética e promover a melhoria contínua dos procedimentos relacionados com a segurança dos dados e informações, para prevenir, detectar e reduzir vulnerabilidades a incidentes relacionados com o ambiente cibernético, assim como possibilitar a manutenção da confidencialidade, da integridade e da disponibilidade das informações sob responsabilidade da empresa. Em 31 de julho de 2018 foi assinado com a EXATUS.net Aditamento aos Contratos de Licenciamentos de Sofwares dos Sistemas SICTUR N. 0017/2017, ASSINANET N. 0035/17.

2. Principais conceitos

A **Segurança Cibernética**, constitui-se da preservação das propriedades da informação, notadamente
sua **confidencialidade**, **integridade** e **disponibilidade**, permitindo o uso e o compartilhamento da informação de forma controlada, bem como do monitoramento e tratamento de incidentes provenientes de ataques cibernéticos, incluindo os controles relacionados aos serviços de nuvem contratados.
Confidencialidade: garantia de que a informação é acessível somente as pessoas autorizadas.
Integridade: salvaguarda da exatidão e dos métodos de processamento da informação.
Disponibilidade: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes, sempre que necessário.
Riscos Cibernéticos: riscos de ataques cibernéticos, internos ou externos, oriundos de malware, técnicas de engenharia social, invasões, ataques de rede (DDos e Botnets), sabotagem, bem como violação de acessos e privacidade, que podem desproteger dados,

redes e sistemas da empresa causando danos financeiros e de reputação ou imagem.

O Aditamento do Contrato de acordo com a Resolução 4.658 26/4/2018 CMN seu Ar. 17, prevê os seguintes serviços relevantes:

i) A indicação dos países e da região em cada País onde os serviços poderão ser armazenados, processados e gerenciados neste caso nossos servidores encontram-se nos Estados Unidos e Canadá;

ii) A adoção de medidas de segurança para a transmissão e armazenamento dos dados citados no inciso I; obrigações constantes na clausula 6 do contrato;

iii) A manutenção, enquanto o contrato estiver vigente, da segregação dos dados e dos controles de acesso para proteção das informações dos clientes;

iv) A obrigatoriedade, em caso de extinção do contrato, de:

a)Transferência dos dados citados no inciso I ao novo prestador de serviços ou à instituição contratante, obrigações constantes na clausula 7.3 do contrato;

b) Exclusão dos dados citados no inciso I pela empresa contratada substituída, após a transferência dos dados prevista na alínea “a” e a confirmação da integridade e da disponibilidade dos dados recebidos, obrigações constantes nas cláusulas 7.3 e 7.4 do contrato;

v) O acesso da instituição contratante a:

a) Informações fornecidas pela empresa contratada, visando a verificar o cumprimento do disposto nos incisos I a III;

b) Informações relativas às certificações e aos relatórios de auditoria especializada, citados no art. 12, inciso II, alíneas “d” e “e”, e

c) Informações e recursos de gestão adequados ao monitoramento dos serviços a serem prestados, citados no art. .12, inciso II, alínea “f”,

vi) A obrigação de a empresa contratada notificar a instituição contratante e sobre a subcontratação de serviços relevantes para a instituição;

vii) A permissão de acesso do Banco Central do Brasil aos contratos e aos acordos firmados para a prestação de serviços, à documentação e às informações referentes aos serviços prestados, aos dados armazenados e às informações sobre seus processamentos, às cópias de segurança dos dados e das informações, bem como aos códigos de acesso aos dados e às informações, são de total responsabilidade do CLIENTE;

viii) A adoção de medidas pela instituição contratante, em decorrência de determinação do Banco Central do Brasil; e

ix) A obrigação de a empresa contratada manter a instituição contratante permanentemente informada sobre eventuais limitações que possam afetar a prestação dos serviços ou o cumprimento da legislação e da regulamentação em vigor, obrigações constantes nas cláusulas 6 e 8 do contrato.

Parágrafo único – O Contrato mencionado no caput deve prever, para o caso de decretação de regime de resolução da instituição contratante pelo Banco Central do Brasil.

I – a obrigação de a empresa contratada conceder pleno irrestrito acesso do responsável pelo regime de resolução aos contratos, aos acordos, à documentação e às informações referentes aos serviços prestados, aos dados armazenados e às informações sobre seus processamentos, às cópias de segurança dos dados e das informações, bem como aos códigos de acesso, citados no inciso VII do caput, que estejam em poder da empresa contratada, obrigações constantes nas cláusulas 7.3 e 7.4 do contrato ; e

II – A obrigação de notificação prévia do responsável pelo regime de resolução sobre a intenção de a empresa contratada interromper a prestação de serviços, com pelo menos trinta dias de antecedência da data prevista para interrupção, observado que:

a) A empresa contratada obriga-se a aceitar eventual pedido de prazo adicional de trinta dias para a interrupção do serviço, feito pelo responsável pelo regime de resolução, e

b) A notificação previa deverá ocorrer também na situação em que a interrupção for motivada por inadimplência da contratante.

3. Gestão de Segurança Cibernética e Informação

A CONEXION possui políticas e procedimentos para assegurar que as informações estejam adequadamente protegidas, baseadas nos requerimentos mínimos exigidos pelos Órgãos Reguladores, nas melhores práticas reconhecidas pelo mercado e Políticas Globais, sendo estabelecidas as seguintes diretrizes:

Gestão de Ativos da Informação: os ativos da informação devem ser identificados de forma individual, inventariados e protegidos de

acessos indevidos, de eventuais adulterações de dados e ter documentação e planos de manutenção atualizados;
Classificação da Informação: as informações devem ser classificadas de acordo com a confidencialidade e as proteções necessárias, abrangendo inclusive a criptografia de dados e de acordo com a classificação dos níveis de relevância: Restrita, Confidencial e Pública;
Gestão de Acessos: as concessões, revisões e exclusões devem basear-se em conceitos de autoridade, autenticidade e privilégios mínimos de acesso. Os acessos devem ser rastreáveis, a fim de garantir a identificação de acesso e transação;
Gestão de Riscos: os riscos devem ser mapeados por meio de um processo estabelecido para análise de vulnerabilidades, ameaças e impactos sobre os ativos de informação, a fim de que sejam endereçadas as proteções adequadas;
Garantia da Continuidade de Negócios: O gerenciamento de riscos deve garantir a manutenção da continuidade dos negócios, abrangendo serviços relevantes e a capacidade de continuar a entrega de produtos ou serviços em um nível mínimo aceitável e previamente definido, quando da ocorrência de um evento que interrompa as operações;
Gestão de incidentes: Os incidentes no âmbito da segurança cibernética, inclusive os ocorridos em sistemas operados ou instalados em empresas contratadas que prestam serviços relevantes, devem ser mantidos em registros organizados, com as respectivas análises de causas e da adoção de controles para minimizar a ocorrência de novos eventos;
Conscientização sobre segurança cibernética: A CONEXION deve garantir a disseminação dos princípios e diretrizes de Segurança cibernética por meio de programas de conscientização e capacitação, fortalecendo a cultura de segurança cibernética e informação, em todos os níveis operacionais.

4. Processamento, armazenamento de dados e computação em nuvem

A CONEXION, quando da utilização de serviços em nuvem, atenderá aos critérios previstos na Resolução 4.658/2018 do CMN, considerando a avaliação de risco que estes representam para o negócio.

5. Responsabilidade e comunicação

O cumprimento da Política de Segurança Cibernética da CONEXION é de responsabilidade de todos os colaboradores e prestadores de serviços, com a abrangência sobre as atividades que envolvam dados e informações no ambiente cibernético.
A alta Administração, compromete-se com a melhoria contínua dos procedimentos e controles relacionados nesta Política.
Quaisquer indícios de incidentes ou irregularidades citadas nesta Política, devem ser comunicadas imediatamente para o departamento de Compliance.

Estará disponível no site em atendimento aos Arts. 4º. e 5º. da Resolução.

A direção da CONEXION em 24/4/2019 com base no aditivo da EXATUS e a Resolução 4.658/CMN estabeleceu as políticas e diretrizes anteriormente definida nesta ATA para adoção na instituição.