## 1.0 PROPÓSITO

Definir os critérios para orientar os colaboradores, clientes, parceiros de negócios e fornecedores referente às melhores práticas a serem adotadas para garantir a segurança cibernética, em conformidade com a legislação vigente e normas internas.

Também estabelece os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem.

## 2.0 APLICAÇÃO

As diretrizes aqui estabelecidas deverão ser seguidas por todos os envolvidos nas operações e processos de negócios, incluindo, mas não se limitando aos colaboradores da área de ICT e aos prestadores de serviços.

## 3.0 POLÍTICA

O gerenciamento de vulnerabilidades é uma parte essencial para garantir a confidencialidade e a integridade das informações e a disponibilidade dos dados e dos sistemas de informação, mantendo a continuidade dos negócios, protegendo nossa reputação e evitando perdas financeiras. Todo esforço deve ser feito para identificar, relatar, priorizar e corrigir adequadamente as vulnerabilidades que representam um risco significativo para o Banco.

O Banco CNH Industrial está comprometido em descobrir e resolver vulnerabilidades de maneira oportuna e ordenada.

A Alta Administração está comprometida com as diretrizes desta política, bem como em apoiar e garantir que estas determinações sejam aplicadas por todos os envolvidos no processo que envolva segurança cibernética.

**Princípios básicos da segurança da informação:**

Os princípios básicos da segurança da informação são: confidencialidade, integridade e disponibilidade das informações. Outra característica é o controle de acesso.

− Confidencialidade: Proteção da informação compartilhada contra acessos não autorizados. Ameaça à segurança acontece quando há uma quebra de sigilo de uma determinada informação, permitindo que sejam expostas voluntaria ou involuntariamente dados restritos e que deveriam ser acessíveis apenas por um determinado grupo de usuários.

− Integridade: Garantia da veracidade da informação, pois a mesma não deve ser alterada enquanto está sendo transferida ou armazenada. Ameaça à segurança acontece quando uma determinada informação fica exposta ao manuseio por uma pessoa não autorizada, que efetua alterações não aprovadas e sem o controle do proprietário (corporativo ou privado) da informação.

- Disponibilidade: Prevenção contra as interrupções das operações da empresa como um todo. Os métodos para garantir a disponibilidade incluem um controle físico e técnico das funções dos sistemas de dados, assim como a proteção dos arquivos, seu correto armazenamento e a realização de cópias de segurança. As ameaças à segurança acontecem quando a informação deixa de estar acessível para quem necessita dela.

− Acesso controlado: O acesso dos usuários à informação é restrito e controlado, significando que só as pessoas que devem ter acesso a uma determinada informação, tenham esse acesso. Ameaça à segurança acontece há descuido ou possível quebra da confidencialidade das senhas de acesso à rede.

**Diretrizes**

a) elaboração de cenários de incidentes considerados nos testes de continuidade de negócios: Considera-se incidente de segurança cibernética qualquer ação que possa comprometer a confidencialidade, integridade, disponibilidade das informações da companhia que possam danificar indivíduos, ameaça à reputação, processos não aderentes órgãos reguladores, afetar os processos negociais e/ou perda financeira.

Os cenários de incidentes que causem a interrupção dos negócios estão descritos no Plano de Continuidade dos Negócios, incluindo o prazo estipulado para reinício ou normalização das suas atividades ou dos serviços relevantes interrompido.

b) definição de procedimentos e de 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: Como política da companhia procura-se minimizar a possibilidade de armazenar e/ou processar dados privados da instituição fora da companhia. Para situações em que se faz necessário este cenário exige-se da empresa prestadora de serviços que seja disponibilizado a sua política interna e procedimentos relativos à estrutura cibernética e tratamento de incidentes bem como a imediata notificação, cooperação e disponibilização de acesso em caso de ocorrência de incidentes que envolvam dados da companhia. Adicionalmente todas as empresas terceiras que prestam serviços para a companhia possuindo acesso a dados de clientes, pagamentos e demais informações sigilosas assinam em contrato termo de confidencialidade declarando que o prestador de serviços e todos os seus funcionários tem ciência deste termo podendo a empresa ser acionada judicialmente em caso de vazamento de informações sigilosas.

c) a classificação dos dados e das informações quanto à relevância: As informações são classificadas nos quesitos: Confidencialidade, integridade e disponibilidade.

**Identificação e comunicação sobre incidentes relevantes:**

Uma das atribuições do gestor de incidente é a divulgação do incidente a todos os envolvidos diretos, assim como o plano de ação e a comunicação de encerramento do incidente com os impactos sofridos, análise de causa e plano de ação para dirimir novos eventos no futuro.

Com a devida comunicação do gestor de incidente, o Banco CNH Industrial comunicará o Banco Central do Brasil das ocorrências de incidentes relevantes e das interrupções dos serviços relevantes, que configurem uma situação de crise pela instituição financeira, bem como das providências para o reinício das suas atividades.

## 4.0 RESPONSABILIDADES

Cabe a todas as áreas envolvidas nas operações e processos de negócios do Banco CNH Industrial a responsabilidade pelo cumprimento e atenção às diretrizes aqui estabelecidas. Cada colaborador é responsável por manter o controle sobre a segurança das informações armazenadas ou disponibilizadas nos equipamentos sob sua responsabilidade.

## 5.0 DEFINIÇÕES

Risco: qualquer evento que possa causar impacto na organização e seus objetivos do negócio;

Ameaça: evento ou atitude indesejável que potencialmente remove, desabilita, danifica ou destrói um recurso ou informação;

Vulnerabilidade: é a fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças;

Incidente: qualquer evento que não faz parte da operação normal de um serviço e que pode causar, ou causa, uma interrupção do serviço ou uma redução de sua qualidade;

Evento: é a ocorrência identificada em um sistema, serviço ou rede que indica uma possível violação da segurança da informação, ou uma situação desconhecida, que passa a ser relevante para a segurança dos ativos;

Ameaças cibernéticas: são tentativas de comprometer a confidencialidade, integridade ou disponibilidade dos dados ou dos sistemas de uma empresa.

## 6.0 CANAL DE COMUNICAÇÃO E DENÚNCIAS:

Denúncias, dúvidas, sugestões ou incidentes relacionados à segurança cibernética do Banco CNH Industrial, constatadas pelo público em geral devem ser comunicadas através do Canal de Denúncias: *www.cnhindustrialcompliancehelpline.com*