CNH CAPITAL

# Política de Segurança Cibernética

## 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 normativos internos e externos.

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 IT e os 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 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.

É terminantemente proibido que os colaboradores façam cópias (físicas ou eletrônicas) ou imprimam os arquivos utilizados, gerados ou disponíveis na rede do Banco e circulem em ambientes externos com estes arquivos, uma vez que tais arquivos contêm informações que são consideradas como confidenciais ou sensíveis, tais como os dados cadastrais e demais informações que permitem a identificação de clientes e suas operações.

### 3.1 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. Garante que somente pessoas autorizadas possam acessar as informações, ou seja, não as torna acessíveis a indivíduos, entidades ou processos não autorizados

− 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.

Autenticidade: é o que firma a verdadeira autoria da informação, que os dados são de fato provenientes de determinada fonte. A autenticidade assegura também o não repúdio, que o autor da informação é incapaz da negação da autoria de tal.

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 quando há descuido ou possível quebra da confidencialidade das senhas de acesso à rede. Os acessos aos sistemas são concedidos de acordo com o disposto no documento: 900101PD001 - Procedimento de Adm Acessos aos Sistemas / NR-GESTÃO DE ACESSOS, provendo a proteção das informações de cadastro e de operações realizadas pelo cliente contra acesso ou destruição não autorizados, vazamento ou adulteração.

**3.2 Procedimentos e controles adotados para reduzir a vulnerabilidade a incidentes:**

A CNH tem estabelecido um conjunto de medidas que contempla a capacidade da instituição para prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados com o ambiente cibernético, incluindo a programação e implementação de controles, na forma abaixo.

**Instalação de *software***

Para garantir que requisitos mínimos de segurança sejam cumpridos em todo o ambiente cibernético da companhia, tais como autenticação, criptografia, segregação de ambientes, todos os softwares devem ser avaliados e validados pela equipe de segurança através de formulário específico

***File server***

O *file server* do Banco CNH é acessado pelos colaboradores mediante login com usuário e senha próprios, tendo os usuários permissões diferenciadas de acordo com as funções e atividades desempenhadas por cada profissional. Dessa forma, os diferentes níveis de permissão viabilizam melhor controle de acesso e de reprodução dos dados e arquivos pelos profissionais do Banco.

***SGBD – AlwaysOn***

O Banco CNH conta com a tecnologia de alta disponibilidade para o Sistema Gerenciador de Banco de dados, onde réplicas dos dados são realizadas *fulltime* para servidor de redundância, mitigando eventuais problemas de indisponibilidade de acesso as informações que venham ocorrer na instancia primaria, isso tudo, em caso de falhas sem nenhum impacto ou percepção visível para os usuários, sendo totalmente transparente e estando sempre disponível.

**Sistema de DR**

Todas as rotinas e principais aplicações *SouthAmerica* foram redesenhadas aumentando o nível tecnológico de segurança em um suposto cenário de desastre nos servidores de aplicação e banco de dados da CNH. Implementados links dedicados e estrutura para outra localidade dentro do Brasil, com sistema DFS para arquivos, réplicas automatizadas e constantes das aplicações, instancia de Database específica incluída no sistema *AlwaysOn*, comunicação direta de arquivos com parceiros (CNH, IVECO, Santander, Bradesco), aumentando assim o nível de segurança em qualquer evento de desastre ou perda dos dados em localidade atual.

**Sistema de confidencialidade dos arquivos**

A CNH implementou um novo sistema de gerenciamento de arquivos integrado com suas ferramentas de trabalho (Outlook, Word, PDF), onde é possível classificar as naturezas dos dados contidos nos arquivos

**Antivírus e Firewall**

A CNH utiliza os serviços de antivírus para se proteger de ameaças cibernéticas, também contamos com um firewall que nos fornece uma barreira de proteção aos nossos serviços e servidores.

**Senhas**

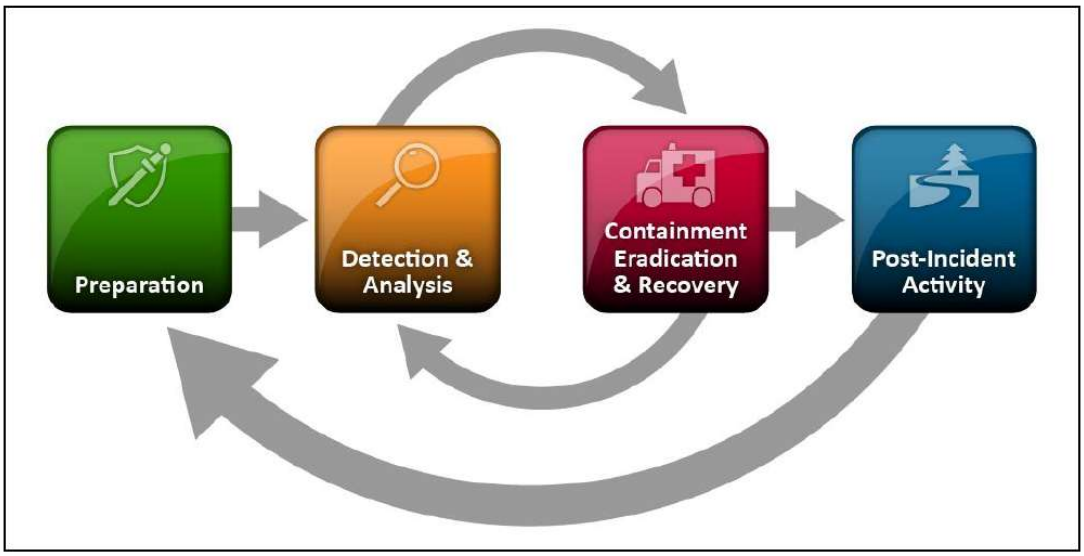
De caráter sigiloso, pessoal e intransferível serão fornecidas aos colaboradores para acesso aos computadores, à rede corporativa e ao correio eletrônico corporativo. Em nenhuma hipótese as senhas poderão ser transmitidas a pessoas que não sejam colaboradores (internos ou terceirizados), sendo os colaboradores responsáveis pela manutenção de cada senha com suas características. Periodicamente os colaboradores são automaticamente obrigados a redefinir suas senhas de acordo com os critérios de segurança estabelecidos pela Companhia.

É proibido o compartilhamento de login para funções de administração de sistemas.

**Monitoramento e testes**

Os mecanismos de supervisão se encontram descritos abaixo, de forma a verificar sua efetividade e identificar eventuais incidentes, detectar as ameaças em tempo hábil, reforçando os controles, caso necessário, e identificar possíveis anomalias no ambiente tecnológico, incluindo a presença de usuários, componentes ou dispositivos não autorizados.

Com o objetivo de detectar, analisar, conter e recuperar qualquer ameaça ao ambiente cibernético da instituição foi criado um plano de resposta a incidentes cibernéticos, que aborda papéis e responsabilidades, classificação de riscos e impactos bem como o ciclo de vida para tratamento de incidentes desde a detecção da ameaça passando pela análise, contenção e erradicação do problema bem como atividades pós-incidente com planos de melhoria contínua e lições aprendidas, conforme pode ser visto na imagem abaixo:




Source: NIST SP 800-61 Figure 3-1.

**3.3 Identificação e atribuição de nível de risco às vulnerabilidades (causa x impacto):**

A companhia leva em consideração os seguintes aspectos para definir a severidade de incidentes:

- Impacto funcional do incidente: Como o incidente irá impactar as funcionalidades existentes nas aplicações afetadas, considerando tanto em situação atual quanto em situação futura, caso o incidente não seja contido.

**Categorias de Impactos de Informação**

| Categoria | Definição |
|---|---|
| N/A | Nenhuma informação foi alterada, excluída ou de outra forma comprometida |
| Violação de Privacidade | Informações Pessoalmente Identificáveis (PII) foram acessadas ou transferidas sem autorização |
| Violação de dados Proprietários | Informações Proprietárias foram acessadas ou transferidas sem autorização |
| Perda de Integridade | Informações sensíveis ou proprietárias foram alteradas ou removidas |

- Impacto de recuperação do incidente: Avaliação do esforço desprendido necessário para recuperação do incidente no quesito tempo e disponibilidade dos recursos afetados.

**Categorias de Impacto de Recuperação de Incidente**

| Categoria | Definição |
|---|---|
| Regular | Tempo de recuperação pode ser estimada com os recursos disponíveis atualmente |
| Suplementada | Tempo de recuperação pode ser estimada com os recursos adicionais |
| Extendida | Tempo de recuperação não pode ser estimada; será necessário recursos adicionais |

| | |
|---|---|
| Não Recuperável | Recuperação do incidente não é possível; iniciar investigação |

Deverá haver o compartilhamento de informações sobre os incidentes relevantes identificados, incluindo informações sobre incidentes relevantes recebidas de empresas prestadoras de serviços a terceiros sem prejuízo do dever de sigilo e da livre concorrência. As informações compartilhadas ficarão disponíveis para o Banco Central do Brasil.

**3.3 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, processos críticos de negócios, dados, informações sensíveis ou disponibilidade das informações da companhia, que tenha impacto significativo sobre os clientes, ameaça à reputação, processos não aderentes aos 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 têm 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: Conforme descrito no documento *Norma – Classificação da Informação,* as informações são classificadas nos quesitos: Confidencialidade, integridade e disponibilidade. Maiores detalhes sobre a classificação de cada quesito acima exposto poderão ser encontrados no item 3.3 do documento ora referenciado.

**3.4 Disseminação da cultura de segurança cibernética:**

Mecanismos para disseminação da cultura de segurança cibernética:

a) O Banco CNH possui um programa de integração de novos Colaboradores no qual o tema sigilo bancário é abordado.
b) Ações para conscientização da importância da segurança da informação são realizadas constantemente para todos colaboradores (Ex: Phishing).
c) Fornecedores são avaliados antes da contratação a fim de garantir o cumprimento dos requisitos de segurança da informação.

d) Conscientização e comunicação via e-mail de boas práticas referente à utilização dos recursos tecnológicos e de novas ferramentas implantadas para auxiliar na segurança dos nossos usuários.
e) A prestação de informações a clientes e usuários sobre precauções na utilização de produtos e serviços financeiros: São disponibilizados avisos de segurança, termos de confidencialidade e demais informações importantes relacionadas a fraudes nos canais diretos que a companhia disponibiliza aos clientes.

**3.5 Identificação e comunicação sobre incidentes relevantes:**

Conforme definido no documento Information Security Incident Response Plan

Uma das atribuições do gestor de incidente do time CERT 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, adicionalmente as informações contidas no documento formalizar a ameça pelos e-mails Time Security Local Latam através do e-mail saictsecurity@cnhind.com e Time Security Global através do e-mail cyberfusioncenter@cnhind.com.

Com a devida comunicação do gestor de incidente do time CERT, o departamento jurídico comunicará o Banco Central do Brasil das ocorrências de incidentes relevantes que gerem impacto no mercado financeiro 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.

**3.6 Contratação de serviços de processamento e armazenamento de dados e de computação em nuvem:**

Previamente à contratação de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem, no Brasil ou no exterior, deverá se certificar, com anuência do time de segurança da companhia que a prestadora de serviço a ser contratada atenda aos requisitos abaixo:

I - A adoção de práticas de governança corporativa e de gestão proporcionais à relevância do serviço a ser contratado e aos riscos a que estejam expostas; e

II - A verificação da capacidade do potencial prestador de serviço de assegurar:

a) o cumprimento da legislação e da regulamentação em vigor;

b) o acesso da instituição aos dados e às informações a serem processados ou armazenados pelo prestador de serviço;

c) a confidencialidade, a integridade, a disponibilidade e a recuperação dos dados e das informações processados ou armazenados pelo prestador de serviço;

d) a sua aderência a certificações exigidas pela instituição para a prestação do serviço a ser contratado;

e) o acesso da instituição contratante aos relatórios elaborados por empresa de auditoria especializada independente contratada pelo prestador de serviço, relativos aos procedimentos e aos controles utilizados na prestação dos serviços a serem contratados;

f) o provimento de informações e de recursos de gestão adequados ao monitoramento dos serviços a serem prestados;

g) a identificação e a segregação dos dados dos clientes da instituição por meio de controles físicos ou lógicos;

h) a qualidade dos controles de acesso voltados à proteção dos dados e das informações dos clientes da instituição; e

I) Comunicação ao Banco Central do Brasil, em até dez dias após a contratação, de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem, assim como alterações contratuais.

III – Caso os recursos disponibilizados pela empresa contratada sejam sediados no exterior, os seguintes requisitos devem ser observados:

a) - a existência de convênio para troca de informações entre o Banco Central do Brasil e as autoridades supervisoras dos países onde os serviços poderão ser prestados;

b) – em caso de inexistência do acordo referido no item a), será necessário solicitar autorização ao Banco Central do Brasil com um prazo de no mínimo sessenta dias antes à contratação e/ou alterações contratuais referentes serviços relevantes de processamento e armazenamento de dados e de computação em nuvem;

c) – assegurar que a prestação dos serviços não cause prejuízos ao regular funcionamento nem embaraço à atuação do Banco Central do Brasil;

d) – definir, previamente à contratação, os países e as regiões em cada país onde os serviços poderão ser prestados e os dados poderão ser armazenados, processados e gerenciados;

e) - prever alternativas para a continuidade dos negócios, no caso de impossibilidade de manutenção ou extinção do contrato de prestação de serviços; e

f) – previsão em contrato das obrigatoriedades:

f.1) transferência dos dados armazenado ao novo prestador de serviços ou à instituição contratante;

f.2) exclusão dos dados pela empresa contratada substituída, após a transferência dos dados prevista na alínea "a" f a confirmação da integridade e da disponibilidade dos dados recebidos; e

f.3) notificar o Banco CNH sobre a subcontratação de serviços relevantes para a instituição.

**3.6.1 Serviços de processamento e armazenamento de dados e de computação em nuvem:**

Considera-se serviço de computação em nuvem os que abrangem a disponibilidade, sob demanda e de maneira virtual, de ao menos um dos seguintes serviços:

I - Processamento de dados, armazenamento de dados, infraestrutura de redes e outros recursos computacionais que permitam à instituição contratante implantar ou executar softwares, que podem incluir sistemas operacionais e aplicativos desenvolvidos pela instituição ou por ela adquiridos;

II - Implantação ou execução de aplicativos desenvolvidos pela instituição contratante, ou por ela adquiridos, utilizando recursos computacionais do prestador de serviços; ou

III - execução, por meio da internet, dos aplicativos implantados ou desenvolvidos pelo prestador de serviço, com a utilização de recursos computacionais do próprio prestador de serviços. Neste caso, deve-se assegurar que o potencial prestador dos serviços adote controles que mitiguem os efeitos de eventuais vulnerabilidades na liberação de novas versões do aplicativo.

3.6.1.1 Considera-se serviços de processamento e armazenamento de dados relevantes todos aqueles que envolvam dados de clientes de crédito ou de captação e informações das respectivas operações.

3.6.2 Das avaliações de contratação e definições para sistemas relevantes.

3.6.2.1 Avaliação de todo tratamento da informação e fluxo de comunicação, observando as políticas de privacidade e segregação de acesso tecnológica, tais como, controles de acesso (permissões e privilégio), rotas de comunicação segura (proxy/firewalls) e utilização/gerenciamento de chaves criptografadas.

3.6.2.2 Avaliação da capacidade do sistema tecnológico em configurações para eventos a serem auditados, rastreados e analisados, também como parâmetros pra detecção de intrusão.

3.6.2.3 Análise do ciclo de alterações e do gerenciamento de mudanças, afim de garantir que se adapta aos controles definidos, que visam garantir a qualidade e a integridade, além de permitir rastrear mudanças autorizadas e prevenir mudanças não autorizadas.

3.6.2.4 Identificação dos itens de configuração para suporte e funcionamento do serviço, tais como requisitos mínimos, versões utilizadas afim de eliminar vulnerabilidades de itens obsoletos.

3.6.2.5 Verificação do processo de criação da mudança, afim de garantir que, exista qualidade e que seja empregado ferramentas para garantir versionamento, testes, homologações antes de aplicação da mudança, garantindo que a politica de segurança para o sistema esteja sendo executada.

Será elaborado por IT BCNH, com suporte da área de IT Cybersecurity responsável por cybersecurity para o grupo CNH, um relatório anual, até 31 de março do ano seguinte conforme previsto na Resolução CMN 4893.

Este relatório deverá ser submetido ao Comitê de Riscos e ao Conselho de Administração.

II - a definição de métricas e indicadores adequados: Disponibilização de relatório mensal contendo o percentual de disponibilidade de sistemas, bem como os chamados de falhas sistêmicas no período.

Geração de relatório anual contendo todos os incidentes cibernéticos ocorridos no ano de forma a validar a correta aplicação do procedimento descrito no documento Global_CNH Information Security – Incident Response Plan, que define o processo de identificação o, tratamento e reporte dos incidentes cibernéticos.

III - a identificação e a correção de eventuais deficiências: Todas as deficiências identificadas, seja pelos testes de segurança, seja por tentativa de ataque real ou por problema reportado por usuário deverá ser prontamente tratado e documentado através de chamados próprios para as equipes envolvidas na deficiência.

Todos os controles e procedimento existentes definidos pela área de IT serão submetidos a testes periódicos pela Auditoria Interna.

## 4.0 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;

Incidente relevante de segurança cibernética: incidente que afete processos críticos de negócios, ou dados ou informações sensíveis, e tenha impacto significativo sobre os clientes;

Serviços relevantes: serviços relacionados aos processos críticos de negócio a que se refere

Sistemas críticos: são todos computadores, redes e sistemas eletrônicos e tecnológicos que se vinculam aos processos críticos de negócios e que diretamente executam ou indiretamente fornecem suporte a funcionalidades cujo mau funcionamento ou indisponibilidade pode provocar impacto significativo nos negócios do intermediário.

Nuvem: rede integrada na internet que oferece serviços de computação com manutenção e recursos efetuados pela empresa contratada.

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