1. INTRODUÇÃO

A Política de Segurança da Informação e Cibernética estabelece diretrizes e normas que permitem aos colaboradores do Banco INDUSCRED, seguirem padrões de comportamento adequados às necessidades do negócio, da proteção legal e do indivíduo no tocante à segurança da informação e cibernética, além de nortear a definição de procedimentos específicos e a implementação de controles e processos para o seu atendimento.

Este documento deve ser lido por todos os colaboradores internos e prestadores de serviços externos ao banco, tendo suas diretrizes respeitadas, haja vista ser um documento normativo e regulatório do banco no que tange ao uso de todos os seus recursos de tecnologia e manuseio de dados para fins de segurança da informação que transita dentro dos processos da instituição.

2. OBJETIVO

O objetivo desta política é definir e projetar a implementação de normas e padrões para proteção de todas as informações que transitam dentro da presente instituição, desde o momento em que é recebida, armazenada e, por fim, disponibilizada. A política de segurança da informação trata principalmente de garantir a confidencialidade de tais informações, manter sua integridade e fazer com que esteja disponível para aqueles autorizados a terem acesso à tais informações.

O Banco Induscred, por se tratar de um banco de investimentos que atua exclusivamente com contratos de crédito concedidos após minuciosa análise de perfil e um tratamento individualizado com seus clientes, o índice de risco em termos de vazamento de informações é baixo, tanto em decorrência da natureza das operações como pelo volume e frequência no trânsito de dados entre o cliente e a instituição.

Sendo assim, o banco possui plena capacidade de armazenar de forma segura as informações dos clientes e em caso de incidentes de vazamento, o risco de que tal informação cause danos relevantes também é bastante baixo, conforme pode ser avaliado no **Item 6.I.C.**

3. DISPOSIÇÕES GERAIS

I. Colaboradores em Geral

A. Toda informação produzida ou recebida pelos colaboradores, sejam internos ou externos, como resultado da atividade profissional contratada pelo Banco Induscred, pertence à referida empresa. As exceções devem ser explícitas e formalizadas em contrato entre as partes;

B. Todos os equipamentos de informática e comunicação, sistemas e informações deverão ser utilizados pelos colaboradores internos e externos para a realização das atividades exclusivamente profissionais;

C. O Banco Induscred reserva-se o direito de monitorar e registrar todo o uso das informações, sistemas e serviços dentro de suas instalações e rede interna;

D. A presente Política de Segurança da Informação e Cibernética deverá ser comunicada a todos os colaboradores internos e externos do Banco Induscred, visando garantir que todas as pessoas tenham consciência da mesma e a pratiquem na empresa;

E. No caso de parceiros, deverá ser comunicada sempre que a parceria envolver acesso aos recursos tecnológicos do Banco Induscred;

F. O uso dos sistemas, recursos tecnológicos, equipamentos e dados do Banco Induscred só poderá ser cedido àqueles que formalizarem a ciência sobre a Política de Segurança da Informação do Banco Induscred e assim comprometendo-se a cumprir fielmente tudo o que está descrito e especificado no presente documento;

G. A presente política de segurança da informação será revisada e atualizada periodicamente, no mínimo a cada ano, ou sempre que algum fato relevante ou evento ocorrer que motive sua revisão antecipada;

H. Deverá constar em todos os contratos do Banco Induscred, o anexo de *Acordo de Confidencialidade, ou cláusula de confidencialidade*, como condição imprescindível para que possa ser concedido o acesso aos ativos de informação disponibilizados pelo Banco;

I. Deverá ser assinado previamente **Acordo de Confidencialidade (Anexo I)** pelos prestadores de serviços e parceiros que recebem informações de projetos para fins de elaboração de orçamento, negociação, propostas, entre outros, que sejam consideradas como relevantes para o negócio do Banco Induscred;

J. O **Plano de Contingência e Continuidade de Negócio (Documento será criado separadamente da presente política)** deve ser implementado e testado, visando reduzir riscos de perda de confidencialidade, integridade e disponibilidade dos ativos de informação, por meio da combinação de ações de prevenção e recuperação. Este plano deverá ser revisado anualmente;

K. A presente Política de Segurança da Informação e Cibernética será implementada no Banco Induscred através de procedimentos específicos a serem desenvolvidos pela gestão de TI e obrigatórios para todos os colaboradores, independentemente do nível hierárquico ou função na empresa, bem como independente de vínculo empregatício ou prestação de serviço e o não cumprimento da mesma acarretará violação às regras internas do banco e sujeitará o usuário às medidas administrativas e legais cabíveis; e

L. Qualquer incidente que venha a ocorrer no tocante à modificação imprevista, perda, roubo ou vazamento de quaisquer informações, sejam elas relacionadas a cliente, colaborador, parceiro ou de uso interno nos sistemas e equipamentos do Banco Induscred, como computadores, servidores e bancos de dados, deverá ser comunicado oficialmente ao Gerente de TI em caráter de urgência, encaminhando email para o endereço **tecnologia@bancoinduscred.com.br.**

II. Recursos Humanos

Cabe aos envolvidos nos processos de Recursos Humanos do Banco Induscred:

A. Atribuir, na fase de contratação dos colaboradores internos e formalizar nos contratos individuais de trabalho, a responsabilidade quanto ao cumprimento da presente Política de Segurança da Informação e Cibernética no Banco Induscred;

B. Colher a assinatura do **Termo de Ciência (Anexo II)** de todos os colaboradores internos e efetuar o arquivamento delas;

C. Quando algum usuário for demitido, solicitar sua demissão, o RH deverá imediatamente comunicar a gestão de TI, a fim de que o acesso seja bloqueado imediatamente, e o login do usuário será mantido por no mínimo 6 (seis) meses para fins de prevenção a

fraude. Esta conduta também se aplica aos colaboradores terceirizados demais e usuários cujo contrato ou prestação de serviços tenham se encerrado, bem como os usuários de testes e outras situações similares. Nestes casos, a comunicação deverá ser realizada pelo Gestor responsável pelo usuário.

III. Diretorias, Gerências e Coordenações

Cabe aos diretores, gerentes e coordenadores do Banco Induscred:

A. Ter postura exemplar em relação à Segurança da Informação, servindo como modelo de conduta para os colaboradores internos sob a sua gestão;

B. Cumprir e fazer cumprir esta política, as normas e procedimentos de Segurança da Informação;

C. Comunicar imediatamente à gestão de TI, eventuais violações da segurança da informação; e

D. Comunicar tempestivamente ao Banco Central todos os incidentes relevantes que causem interrupção nas operações ou serviços.

IV. Tecnologia da Informação

Cabe ao gerente e à equipe da área de Tecnologia da Informação do Banco Induscred:

A. Manter testes constantes da eficácia dos controles de segurança da informação e comunicar por meio de relatórios oficiais os diretores e coordenadores do banco mensalmente;

B. Gerenciar o acesso aos dados e recursos computacionais por meio de permissões administrativas, permitindo o uso somente daquilo que for estritamente necessário para o trabalho diário dos colaboradores e envolvidos nas tarefas do Banco Induscred;

C. Gerar e manter as trilhas para auditoria com nível de detalhe suficiente para rastrear possíveis falhas e fraudes. Para as trilhas geradas e/ou mantidas em meio eletrônico, implantar controles de integridade de forma a torná-las juridicamente válidas como evidências;

D. Planejar, implantar e monitorar a capacidade de armazenamento, processamento e transmissão, necessárias para garantir a segurança e eficiência requerida pelas áreas de negócio;

E. Atribuir cada conta ou dispositivo de acesso a computadores, sistemas, bases de dados e a qualquer outro ativo de informação a um responsável identificável como pessoa física;

F. Proteger continuamente todos os ativos de informação da empresa contra código malicioso;

G. Garantir que todos os novos ativos da informação da empresa só entrem para o ambiente de produção após estarem livres de código malicioso e/ou indesejado;

H. Definir as regras formais para instalação de Software e Hardware em ambiente de produção corporativo;

I. Realizar auditorias periódicas de configurações técnicas e análise de riscos;

J. Monitorar o ambiente de TI, gerando indicadores diversos de uso, performance, eficiência e estabilidade, a fim de garantir o bom desempenho dos trabalhos de todos os colaboradores;

K. Publicar e promover as versões da Política de Segurança da Informação e Cibernética aprovadas pela Diretoria Administrativa em canal oficial na rede interna do Banco Induscred;

L. Promover campanhas, palestras e treinamentos dos colaboradores internos, externos e parceiros em relação à Segurança da Informação para o negócio do banco; e

M. Manter comunicação efetiva com a Diretoria Administrativa, com o objetivo de mantê-los adequadamente informados sobre assuntos relacionados ao tema, que afetem ou tenham potencial para afetar o Banco Induscred.

4. PROCEDIMENTOS GERAIS DE SEGURANÇA DA INFORMAÇÃO

Os procedimentos gerais de segurança da informação tratam das medidas gerais e iniciais adotadas no plano da política de segurança da informação, sendo assim, não estão relacionados diretamente a qualquer processo interno ou dispositivo, mas são importantes para todas as estruturas como um ponto de partida essencial para a segurança da informação.

I. Política de senhas fortes

O Banco Induscred aplica uma política de senhas fortes para todos os terminais locais de trabalho, servidores, bancos de dados e outros sistemas de terceiros que exijam autenticação, a qual respeita as seguintes regras:

- Ter ao menos 8 caracteres;
- Ter no mínimo 2 letras maiúsculas;
- Possuir caracteres numéricos e alfabéticos; e
- Utilizar pelo menos 2 símbolos (Ex.: !, @, #, $, %, &, etc.).

II. Rotina de renovação de senhas

Deve ser aplicada no Banco Induscred uma rotina de renovação de senhas que ocorre a cada 3 meses (90 dias), onde não se poderá utilizar senhas utilizadas anteriormente, bem como os sistemas deverão forçar essa renovação.

III. Suspensão da sessão do terminal quando ausente

É exigido de todos os colaboradores que estando ausente do seu terminal de trabalho, seja para quaisquer fins, deve suspender sua sessão no sistema operacional, de forma que sua área de trabalho fique protegida pela tela de solicitação de autenticação do terminal de trabalho.

Obs.: Atualmente, todos os terminais de trabalho utilizam o sistema operacional Windows, o qual dispõe do recurso de suspender a sessão de trabalho do usuário, bloqueando a tela com uma solicitação de autenticação.

IV. Acesso à sala de servidores

A sala dos servidores é uma área de acesso exclusivo da equipe de TI responsável pela manutenção dos servidores e equipamentos de rede e segurança de rede. O local deve estar trancado, refrigerado por ar-condicionado em temperatura adequada aos equipamentos e estes devem estar acondicionados em armários específicos para computadores, servidores e equipamentos de rede **(Anexo III)**.

O acesso à sala dos servidores somente poderá ser franqueado com o acompanhamento do Gerente de TI do Banco Induscred ou alguém diretamente indicado por este, mediante o preenchimento de registro digital de visita, contendo data, horário de entrada e saída do local, a qualificação do visitante e indicação dos procedimentos que realizará. Este registro digital é feito por meio da plataforma Trello **(Anexo IV).**

V. Atualizações de software

Todos os meses devem ser feitas varreduras em todos os softwares utilizados pelo Banco Induscred, para averiguação de suas atualizações, de forma que deve-se manter todos os sistemas em suas versões mais atuais possível, desde que tais atualizações não sejam empecilho para o desempenho dos trabalhos da instituição.

Sendo assim, as atualizações de sistemas operacionais, seja em terminais locais de trabalho ou servidores, sistemas de bancos de dados, softwares de gestão e outras aplicações utilitárias devem ser analisadas pela equipe de TI, ter tempo específico e definido para que sejam aplicadas tais atualizações, sempre respeitando um fluxo de atualização que se inicia em ambiente de homologação e somente depois de feitos todos os testes necessários, será feita a implementação das atualizações em servidores de produção.

O fluxo de atualização de software seguirá o seguinte procedimento:

1. Avaliação dos arquivos e procedimentos envolvidos na atualização a ser feita;
2. Averiguação de possibilidade de software malicioso;
3. Procedimento de atualização em ambiente de homologação;
4. Testes de funcionalidade e interação com outros sistemas;
5. Comunicado em canal oficial do Banco Induscred sobre período de atualização de sistemas;
6. Aguardar aceite de todos os envolvidos e possíveis impactados por paralisações de sistemas;
7. Execução de medidas preventivas antes de executar as atualizações, como backups de pastas, bancos de dados, armazenamento em HDs externos apropriados, etc.;
8. Procedimento de atualização em ambiente de produção; e
9. Testes finais em ambiente de produção e possíveis ajustes.

VI. Acesso aos sistemas da Autbank

O sistema Autbank, software de gestão bancária utilizado por vários colaboradores do Banco Induscred em suas funções diárias, deve ser acessado tão somente por estes colaboradores que necessitam fazer uso de seus recursos, utilizando sempre um conjunto de autenticação (login e senha) único e exclusivo cedido ao colaborador, não sendo permitido o compartilhamento dessas informações de acesso com outros colaboradores ou terceiros.

No caso de uma possível dificuldade de acesso de algum colaborador ao seu próprio ambiente dentro do sistema Autbank, o departamento de tecnologia do Banco Induscred deve ser notificado por meio do email **tecnologia@bancoinduscred.com.br**, o qual dará as tratativas necessárias para o restabelecimento do acesso do colaborador ao sistema da Autbank e o retorno às suas atividades normais.

VII. Acesso remoto aos terminais e servidores

Ocorre em muitas ocasiões de suporte técnico por parte de prestadores de serviços externos o acesso remoto à servidores e terminais locais de trabalho. Nessas ocasiões, é obrigatório que um dos membros da equipe de TI do Banco Induscred faça a liberação do acesso e o acompanhamento de todas as ações realizadas pelo operador remoto, sendo capaz de mitigar qualquer ação suspeita ou equivocada que possa trazer danos aos sistemas, dados e rede interna do banco.

VIII. Diretrizes para Proteção das Informações

Por força da Lei 13.709/2018 - Lei Geral de Proteção de Dados Pessoais, e suas alterações, o Banco INDUSCRED deverá manter as informações cadastrais de seus clientes, fornecedores, parceiros comerciais e colaboradores, sejam funcionários ou terceiros, protegidas quanto a vazamentos e divulgação de dados pessoais, quer de forma intencional ou involuntária.

Os documentos mantidos em arquivos físicos, deverão permanecer em armários trancados de forma a impedir o acesso por pessoas não autorizadas.

Os documentos mantidos em arquivos digitais, quando arquivados na rede local, deverão possuir controle de acesso apenas aos usuários autorizados a consultar as informações. Quando arquivados em aplicações na nuvem (ex.: OneDrive, Dropbox, Google Drive) deverá haver restrição de acesso apenas aos usuários autorizados a consultar informações.

O acesso às pastas de documentos, mantidas em arquivo digital, somente será realizado mediante identificação do usuário com login na rede e monitorado pela tecnologia.

É terminantemente proibida a divulgação, reprodução ou comercialização de informações do cadastro de clientes, tanto de pessoas jurídicas, quanto de pessoas físicas.

5. PROCEDIMENTOS DE SEGURANÇA APLICADOS AOS PROCESSOS INTERNOS E DISPOSITIVOS RELACIONADOS

Os procedimentos de segurança da informação aplicados aos processos e dispositivos trata das ações preventivas, manutenções, avaliações periódicas e do gerenciamento de incidentes que devem ser implementados sobre os processos internos do Banco Induscred, considerando-se nesta implementação os dispositivos envolvidos em cada um destes processos, como servidores, bancos de dados, terminais locais de trabalho, softwares, etc.

I. Bancos de Dados

O Banco Induscred utiliza hoje dois servidores de bancos de dados, sendo um para testes e homologação e outro para a realização do trabalho normal do banco (servidor de produção), onde ficam armazenados os dados utilizados pelo sistema Autbank.

A. Máquinas virtuais, isolamento dos servidores e acesso por VPN

Para que tenhamos maiores garantias da segurança dos dados armazenados nos bancos de dados, ambos estão instalados dentro de máquinas virtuais criadas em servidores dedicados, os quais estão fisicamente separados e isolados um do outro e só podem ser acessados por meio de VPN, um canal que torna o acesso ainda mais seguro do que se fosse feito de forma direta no próprio servidor **(Anexo V)**.

B. Atualizações

Utilizamos como sistema de banco de dados o Microsoft SQL Server, o qual deve-se manter atualizado conforme novas atualizações e patches corretivos são disponibilizados pela fabricante (Microsoft). Para isso, a equipe de TI deve ser diligente em atentar para as notícias sobre atualizações e patches de correção que a fabricante publica em seu site oficial **(Anexo VI)**.

C. Permissão de manuseio dos bancos de dados

O manuseio dos bancos de dados é permitido somente aos profissionais de TI do Banco Induscred, os quais estão devidamente habilitados a manusear e dar manutenção nestes sistemas, bem como executar scripts que estejam livres de ações maliciosas e que possam comprometer de alguma forma o bom funcionamento das aplicações do banco ou mesmo gerar algum tipo de falha na manutenção dos dados, comprometendo, assim, a confidencialidade e a integridade deles.

D. Execução de scripts SQL

A execução de scripts nos bancos de dados está exclusivamente reservada para os profissionais de TI do Banco Induscred, os quais somente deverão executar scripts após minuciosa avaliação de seu conteúdo e permissão expressa do Gerente de TI da instituição.

A execução de scripts SQL deve ser feita somente em caso de absoluta necessidade para que os sistemas do banco mantenham-se funcionais e deve seguir o seguinte procedimento:

1. Recepção do script no email **tecnologia@bancoinduscred.com.br;**
2. Cadastro da tarefa de execução de script na ferramenta de gestão de projetos Trello **(Anexo VII)**;
3. Leitura e auditoria do conteúdo do script com aprovação do Gerente de TI;
4. Backup do banco de dados de homologação e produção;
5. Execução do script em banco de dados de homologação;
6. Testes e avaliação do resultado;
7. Execução do script em banco de dados de produção;
8. Testes e avaliação do resultado; e
9. Encerramento da tarefa na ferramenta de gestão de projetos (Atlassian Trello).

E. Backups

Todos os dias será feito um backup integral do banco de dados de produção e uma vez por semana deverá ser feito um backup integral do banco de dados de homologação.

Todos os backups dos bancos de dados serão salvos em arquivos SQL, pois nesse formato os scripts podem ser analisados, testados e posteriormente utilizados com mais facilidade para a reconstrução do banco de dados em algum ponto específico.

Os arquivos de backup gerados deverão ser armazenados em HD externo apropriado, o qual ficará guardado e armazenado em armário especificamente destinado à guarda de equipamentos eletrônicos na sala dos servidores.

Além disso, é de suma importância que estes backups estejam em pastas organizadas por data (padrão americano). Por exemplo, um arquivo SQL extraído do banco de dados de produção deve seguir o seguinte padrão para ser armazenado e nomeado:

2021 *(ano)*
|___ 06 *(mês)*
|___ backup-database-producao-2021-06-12.sql (arquivo de backup integral)

F. Versionamento

Após a realização do backup integral diário do banco de dados de produção e do backup integral semanal do banco de dados de homologação, estes arquivos deverão ficar em uma pasta dentro do servidor, a qual terá uma comunicação com a plataforma em nuvem Bitbucket, pertencente à empresa Atlassian, por onde estes arquivos poderão ser enviados para um sistema de repositório de códigos em nuvem, o qual irá gerar uma numeração de versão para tais arquivos no momento da sincronização.

Sendo assim, fica a cargo de um ou mais profissionais de TI a responsabilidade de todos os dias realizar o backup do banco de dados e fazer o versionamento do arquivo SQL, armazenando-o no repositório da plataforma Atlassian Bitbucket.

Este versionamento permite que possamos ter acesso dentro de uma escala temporal aos diversos momentos dos bancos de dados, além de nos permitir recuperar o banco de dados em um determinado ponto no tempo.

G. Atividades proibidas

Segue abaixo atividades proibidas no tocante aos bancos de dados:

- Armazenar informações não pertinentes aos negócios do Banco Induscred;
- Utilizar os bancos de dados sem ser pessoa autorizada diretamente pelo Gerente de TI; e
- Executar scripts sem autorização do Gerente de TI e/ou sem realizar o processo adequado para execução de scripts nos bancos de dados, o qual está descrito no **item 5.I.D.** da presente Política de Segurança da Informação.

H. Avaliação Periódica de Segurança

Duas vezes por mês (a cada quinze dias), serão realizados testes de segurança nos bancos de dados (homologação e produção), conforme segue:

- Teste de acesso não autorizado aos servidores onde estão os bancos de dados;
- Teste de acesso aos bancos de dados por rede externa sem uso de VPN;
- Avaliação da estabilidade dos servidores quando sob alta carga de processos;

- Avaliação de performance quando executados scripts que exijam uma grande carga de processamento;
- Reconstrução dos dois bancos de dados a partir de backups feitos em dias aleatórios;
- Tentativa de execução de scripts maliciosos no banco de dados (SQL Injection);
- Averiguação e revisão dos usuários e permissões vigentes; e
- Testes de integridade dos dados (dados de clientes, contabilidade, contas, etc.).

II. E-mail

As contas de email institucional do Banco Induscred devem ser criadas somente para colaboradores envolvidos diretamente nos trabalhos diários do banco e para os quais tal conta de email tenha utilidade para a execução destes trabalhos.

Satisfeita esta condição, a criação de uma conta de email deve ser sempre feita mediante solicitação do colaborador ao Gerente de TI, o qual providenciará a criação da conta e dará as instruções para configuração e uso da conta no terminal local de trabalho do colaborador.

O uso do email pelo colaborador deve obedecer ao que está estabelecido no *Acordo de Confidencialidade,* o qual deve já estar assinado pelo colaborador.

A. Atividades proibidas

Fica explicitamente proibido a todos os colaboradores o uso de email para as seguintes situações:

- Enviar mensagem por correio eletrônico a partir do endereço de seu departamento ou usando o nome de usuário de outra pessoa ou endereço de correio eletrônico que não seja de seu próprio usuário;
- Enviar qualquer mensagem através dos meios eletrônicos que torne seu remetente e/ou o Banco Induscred ou suas subsidiárias vulneráveis a ações civis ou criminais;
- Divulgar informações não autorizadas ou imagens de tela, sistemas, documentos e afins sem autorização expressa e formal concedida pelo proprietário deste ativo de informação;
- Falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários;
- Produzir, transmitir ou divulgar mensagem que:
    - Contenha qualquer ato ou forneça orientação que conflite ou contrarie os interesses do Banco Induscred;
    - Contenha ameaça eletrônica de qualquer tipo;
    - Inclua imagens criptografadas ou de qualquer forma mascaradas;
    - Tenha conteúdo considerado impróprio, obsceno ou ilegal;
    - Seja de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico etc.; e
    - Inclua material protegido por direitos autorais sem a permissão do detentor dos direitos.

B. Avaliação Periódica de Segurança

Uma vez por mês, todas as contas de email dos colaboradores do Banco Induscred passará por manutenção, onde serão avaliados os seguintes quesitos:

- Espaço de armazenamento;
- Velocidade de recebimento e envio;
- Respeito às regras de email criadas e criação de pastas personalizadas;
- Estabilidade do serviço;
- Varredura em busca de conteúdo malicioso, confidencial ou não condizente com a presente política de segurança da informação que possa ter sido enviado ou recebido pelo colaborador; e
- Teste de ferramenta de detecção de spams.

III. Terminais locais de trabalho

A. Antivírus

Para que tenhamos um bom nível de segurança nos terminais locais de trabalho, todos eles contarão com uma licença de software antivírus instalado, o qual será mantido atualizado pela equipe de TI.

B. Senha de acesso

Cada terminal de trabalho possuirá uma senha exclusiva para acesso, a qual deve ser de conhecimento somente da equipe de TI e do próprio colaborador que utiliza o terminal de trabalho, não podendo ser comunicada a outros colaboradores ou terceiros, bem como deverá ser atualizada a cada 3 meses (90 dias).

C. Instalação de softwares

A instalação de softwares nos terminais locais de trabalho está proibida e bloqueada para os usuários não administradores, sendo reservada a permissão de instalação somente aos usuários administradores dos sistemas internos do Banco Induscred, os quais são profissionais de TI qualificados para a realização destas instalações com segurança, evitando o risco de que o terminal local, bem como a rede interna sejam infectados com vírus e outros tipos de ameaças digitais que por vezes acompanham softwares vindos da internet ou de locais desconhecidos.

Para a instalação de qualquer software em qualquer computador nas dependências do Banco Induscred, esta instalação deve ser solicitada pelo colaborador por meio do envio de um e-mail para o endereço **tecnologia@bancoinduscred.com.br**, sendo avaliada a viabilidade, utilidade e segurança desta instalação e somente no caso de ser viável, útil e segura, bem como aprovada pelo profissional de TI, a instalação poderá ser realizada.

D. Arquivos pessoais

Não é recomendado que arquivos pessoais sejam deixados armazenados nos terminais de trabalho pelos seguintes motivos:

- Se porventura forem perdidos, o banco não se responsabilizará por tal evento;

- Ocuparão espaço de armazenamento no computador local, diminuindo sua total eficiência voltada para o trabalho que deve ser desempenhado no banco; e
- Arquivos pessoais não serão auditados pela equipe de tecnologia, logo, podem comprometer a segurança do computador local e da própria rede interna do banco no caso de serem arquivos que contenham algum comportamento malicioso, sendo que, neste caso, o colaborador, dono dos arquivos maliciosos, irá se responsabilizar pelos danos ocorridos ao computador, à rede interna e quaisquer outros danos decorrentes dos arquivos pessoais que armazenou.

E. Atividades proibidas

Fica explicitamente proibido a todos os colaboradores o uso de computadores e recursos tecnológicos do Banco Induscred para as seguintes situações:

- Tentar obter acesso não autorizado a outro computador, servidor ou rede;
- Burlar quaisquer sistemas de segurança, internos ou externos ao banco;
- Acessar informações confidenciais sem explícita autorização do proprietário;
- Vigiar secretamente outrem através de dispositivos eletrônicos ou softwares;
- Interromper um serviço, servidor ou rede de computadores através de qualquer método;
- Usar qualquer tipo de recurso tecnológico para cometer ou ser cúmplice de atos de violação, assédio sexual, perturbação, manipulação ou supressão de direitos autorais ou propriedades intelectuais sem a devida autorização legal do titular;
- Hospedar pornografia, material racista ou qualquer outro que viole a legislação em vigor no país, a moral, os bons costumes e a ordem pública;
- A utilização de recursos de terceiros em conjunto com recursos tecnológicos do banco. (Ex.: pendrive pessoal ou do cliente/parceiro, smartphones, tablet etc.); e
- Utilizar software sem licença oficial do fabricante.

F. Avaliação Periódica de Segurança

Duas vezes por mês (a cada quinze dias), todos os terminais locais de trabalho passarão por manutenção periódica avaliando os seguintes tópicos:

- Atualização do Sistema Operacional (Windows);
- Averiguação das aplicações instaladas com remoção de qualquer aplicação indevida;
- Varredura do sistema pelo antivírus;
- Limpeza de cache, pastas temporárias e liberação de memória alocada não liberada com uso de software de limpeza;
- Avaliação de desempenho (memória) e armazenamento (HD);
- Avaliação dos acessos às impressoras e à rede interna do Banco Induscred;
- Atualização de drivers; e
- Testes de entrada no sistema com usuário não permitido.

IV. Sistema Autbank

O sistema Autbank deve ser utilizado somente pelos colaboradores envolvidos em atividades para as quais o sistema se mostre útil, sendo que cada um destes colaboradores terá seus próprios dados de acesso (email e senha), os quais não devem ser compartilhados com nenhum outro colaborador, terceiro ou cliente, bem como deverá ser aplicada a política de senhas fortes e renovação periódica de senhas para a senha de acesso ao Autbank, conforme descrito nos **itens 4.I e 4.II** da presente Política de Segurança da Informação.

A. Atualizações

- As atualizações do sistema Autbank devem sempre ser enviadas para o email **tecnologia@bancoinduscred.com.br**, a qual deverá passar por avaliação e ser aprovada pelo Gerente de TI antes de ser instalada;
- As atualizações poderão ser feitas por qualquer profissional do departamento de tecnologia do Banco Induscred, desde que este esteja devidamente autorizado pelo Gerente de TI;
- As atualizações deverão sempre ser cadastradas no sistema de acompanhamento de processos internos do departamento de TI. Atualmente, a equipe de TI do Banco Induscred faz uso da plataforma online **Trello** da empresa **Atlassian,** por onde a equipe de TI pode verificar o andamento das atualizações e todas as outras demandas do departamento; e
- Caso a atualização exija paralisação do sistema Autbank, deverá ser seguido o procedimento de atualização de software descrito no **Item 4.IV** da presente Política de Segurança da Informação.

B. Scripts SQL

Nos casos em que se deva executar scripts SQL no banco de dados onde estão armazenados os dados do sistema Autbank, deve-se seguir o procedimento de execução de scripts descrito no **Item 5.I.D.** da presente Política de Segurança da Informação.

C. Backups

Uma vez por semana será feito um backup integral dos arquivos do sistema Autbank, tanto os arquivos do servidor de homologação como os do servidor de produção.

Os arquivos de backup gerados deverão ser armazenados em HD externo apropriado, o qual ficará guardado e armazenado em armário especificamente destinado à guarda de equipamentos eletrônicos na sala dos servidores.

Além disso, é de suma importância que estes backups estejam em pastas organizadas por data (padrão americano). Por exemplo, arquivos WAR devem seguir o seguinte padrão para ser armazenado e nomeado:

2021 *(ano)*
|___ 06 *(mês)*
|___ deploy *(arquivos para execução do deploy)*
| |___ backup-autbank-producao-2021-06-12.war (arquivo de backup binário)
|___ www *(arquivos da aplicação web)*
|___ backup-autbank-producao-2021-06-12.zip (arquivo compactado com os arquivos da aplicação web)

D. Versionamento

Após a realização do backup integral semanal do sistema Autbank e de seu armazenamento em HD Externo, estes arquivos deverão ficar em uma pasta dentro do servidor, a qual terá uma comunicação com a plataforma em nuvem Bitbucket, pertencente à empresa Atlassian, por onde estes arquivos poderão ser enviados para um sistema de repositório em nuvem, o qual irá gerar uma numeração de versão para tais arquivos no momento da sincronização.

Sendo assim, fica a cargo de um ou mais profissionais de TI a responsabilidade de todas as semanas realizar o backup do sistema Autbank e fazer o versionamento dos arquivos, armazenando-os no repositório da plataforma Atlassian Bitbucket (Git).

Este versionamento permite que possamos ter acesso dentro de uma escala temporal aos diversos momentos do sistema, além de nos permitir recuperar o sistema em um determinado ponto no tempo.

E. Atividades proibidas

Fica explicitamente proibido a todos os colaboradores o uso do sistema Autbank das seguintes formas:

- Utilizar algum dos subsistemas em que não esteja habilitado para o uso ou que não esteja relacionado à função do colaborador dentro do banco;
- Acessar o sistema com dados de autenticação de outro colaborador;
- Compartilhar por qualquer meio com terceiros que não estejam envolvidos diretamente nos trabalhos do banco os dados armazenados no sistema;

F. Avaliação Periódica de Segurança

Uma vez por mês será feita uma avaliação periódica de segurança no sistema Autbank, aplicando testes conforme segue:

- Reconstruir a instalação do sistema a partir de um dos backups, o qual deve ser escolhido aleatoriamente em algum ponto no passado dentro da plataforma Atlassian Bitbucket;
- Tentar acessar usuários com senhas incorretas para ver se o sistema trava o acesso;
- Testar a estabilidade e performance do sistema quando for estressado com tarefas que exijam alta demanda de processamento;
- Verificação de todos os subsistemas, avaliando se estão acessíveis, funcionais e com performance adequada para que os trabalhos do banco ocorram normalmente;
- Verificar se todas as atualizações recebidas da fabricante foram realizadas; e
- Verificar junto à equipe da Autbank se todos os arquivos de atualização foram enviados e caso falte algum arquivo, solicitar e implementar conforme procedimento de atualização descrito no **Item 5.IV.A** da presente Política de Segurança da Informação.

6. REGISTRO DE INCIDENTES

O Banco Induscred realiza a apuração do Risco Operacional, controlado sistemicamente, no qual estão mapeados todos os processos internos do banco, calculados os níveis de risco de cada processo, definidos os planos de ação e mitigação em incidentes, bem como onde todos os incidentes são registrados e estão disponíveis para serem auditados por meio de relatórios que o próprio sistema fornece.

Todos os relatórios de incidentes e os mapas dos processos internos estão disponíveis para consulta dos diretores do Banco Induscred, auditorias internas e externas, bem como órgãos reguladores competentes e o Banco Central do Brasil.

I. Diretrizes

A. Elaboração de cenários de incidentes

Os cenários de incidentes serão montados com base nas situações mais comuns no dia a dia do banco, além de todos os meses fazer um levantamento com os colaboradores sobre os incidentes mais comuns para que possamos simular uma situação em que se estressa o sistema diante de tal cenário e com base nos resultados avaliarmos se há a necessidade de novas configurações e tratativas nos processos, sistemas e dispositivos de tecnologia do Banco Induscred.

Os testes de continuidade de negócios estão descritos no documento **Plano de Contingência e Continuidade de Negócio (Documento será criado separadamente da presente política).**

B. Padrões de segurança exigidos de prestadores de serviços a terceiros

Todos os prestadores de serviços a terceiros envolvidos com o Banco Induscred, no momento de sua contratação devem assinar o *Acordo de Confidencialidade*, bem como executar seus serviços somente acompanhado por um profissional de TI qualificado e designado pelo Gerente de TI do Banco Induscred, seja para executar acessos remotos em terminais internos para fins de suporte técnico, seja presencialmente nas instalações do Banco Induscred.

C. Classificação dos dados e informações quanto à relevância

O Banco Induscred armazena e manipula dados diversos, os quais são classificados em três níveis de relevância: Baixa, Média, Alta. Tal classificação diz respeito à extensão dos danos que um possível vazamento destes dados pode causar ao titular dos dados e ao próprio banco, bem como a dificuldade de rastreio e recuperação deles.

- Dados pessoais de clientes
  Relevância da informação: Alta
- Informações descritivas de pessoas jurídicas relacionadas a clientes
  Relevância da informação: Média
- Informações do cliente constantes no Sistema de Informações de Créditos (SCR)
  Relevância da informação: Alta
- Dados pessoais de colaboradores
  Relevância da informação: Alta

- Informações descritivas de pessoas jurídicas relacionadas a colaboradores
  Relevância da informação: Média
- Dados financeiros e patrimoniais relacionados a clientes (pessoas físicas e jurídicas)
  Relevância da informação: Alta
- Contratos de crédito
  Relevância da informação: Média
- Informações de investimento de clientes
  Relevância da informação: Média
- Dados armazenados pelo sistema Autbank para seu funcionamento (taxas, cálculos, parâmetros de sistema, etc.)
  Relevância da informação: Baixa
- Dados contábeis e administrativos internos do Banco Induscred
  Relevância da informação: Baixa

D. Parâmetros para avaliação da relevância de incidentes

Os parâmetros utilizados para avaliação da relevância de incidentes no Banco Induscred inspiram-se no procedimento adotado pela Agência Espanhola de Proteção de Dados Pessoais, a qual define o seguinte quanto à relevância de incidentes com dados pessoais:

- Quais são as obrigações legais e contratuais;
- Quais são os riscos decorrentes da perda dos dados pessoais: Ex.: danos materiais, danos reputacionais etc.;
- Se existe risco razoável de falsificação de identidade ou fraude (em razão do tipo de informação afetada e levando em consideração se a informação foi pseudonimizada ou criptografada); e
- Até que ponto a pessoa afetada pode evitar ou mitigar possíveis danos posteriores.

Avaliando tais perguntas, buscamos apurar para cada tipo de informação qual sua classificação dentre as quatro utilizadas, conforme já apresentado no item anterior.

7. SEGURANÇA CIBERNÉTICA COMO CULTURA CORPORATIVA

As práticas, normas e procedimentos de segurança da informação até aqui expostos dependem em grande medida do bom uso dos sistemas internos do Banco Induscred por parte dos colaboradores e terceiros.

Sendo assim, em atendimento ao solicitado pelo Banco Central do Brasil e para que a presente Política de Segurança da Informação seja conhecida, bem interpretada e praticada, o departamento de TI do Banco Induscred propõe as seguintes ações:

- Palestra sobre Segurança da Informação e temas relacionados, como LGPD, PLD, Compliance, Hacking, Fraudes, etc., 1 vez a cada 2 meses (a cada 60 dias);
- Publicação constante de artigos técnicos, notícias relevantes e manuais com orientações sobre procedimentos de segurança em portal de conteúdo dentro da rede interna do Banco Induscred;

- Treinamento em Segurança da Informação e boas práticas de uso dos dispositivos de tecnologia a cada 6 meses para os colaboradores e prestadores de serviços a terceiros do Banco Induscred; e
- Envio de comunicações por email institucional aos colaboradores, prestadores de serviços e clientes sobre atualizações das normas e procedimentos de segurança, bem como reciclando constantemente informações relevantes para manter o bom nível de segurança das informações da instituição.

8. DISPOSIÇÕES FINAIS

- A qualquer tempo e em qualquer dos casos previstos, prevalecendo o descumprimento das regras expostas, a gestão de TI poderá bloquear temporariamente o acesso do colaborador comunicando a ele e ao gestor da área os motivos de tal ato. No caso de colaborador externo deverá ser comunicado ao responsável da empresa terceirizada;
- Esta Política de Segurança da Informação compromete e responsabiliza cada um, estando todos cientes também que os ambientes, telefones, sistemas, e-mails, computadores e redes do banco estão sujeitos a monitoramento e gravação;
- É também obrigação de cada colaborador se manter atualizado quanto ao texto da presente Política de Segurança da Informação e aos procedimentos e normas relacionadas, buscando orientação do seu gestor ou da gestão de TI, sempre que não estiver absolutamente seguro quanto à aquisição, uso e/ou descarte de informações; e
- O colaborador assume o compromisso de não utilizar, revelar ou divulgar a terceiros, de modo algum, direta ou indiretamente, em proveito próprio ou de terceiros, qualquer informação, confidencial ou não, que tenha ou venha a ter conhecimento em razão de suas funções no Banco Induscred, mesmo depois de terminado o vínculo contratual mantido com a instituição, conforme consta no *Acordo de Confidencialidade*.

9. BASE NORMATIVA

- **Resolução CMN nº 4.893 de 26 de fevereiro de 2021** – Dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil;
- **ISO 27001** - é um padrão para sistema de gestão da segurança da informação (ISMS - Information Security Management System) publicado em outubro de 2005 pelo International Organization for Standardization e pelo International Electrotechnical Commission. O seu nome completo é ISO/IEC 27001- Tecnologia da informação - técnicas de segurança - sistemas de gestão da segurança da informação - requisitos, mais conhecido como ISO 27001.
- **ISO 27032** - é um padrão para sistema de gestão da segurança da informação (ISMS - Information Security Management System) publicado em outubro de 2015 pelo International Organization for Standardization e pelo International Electrotechnical Commission. O seu nome completo é ISO/IEC 27032 - Tecnologia da Informação — Técnicas de segurança — Diretrizes para segurança cibernética Information technology — Security techniques — Guidelines for cybersecurity.

10. ANEXOS

Anexo I. Acordo de Confidencialidade e Segurança da Informação

ACORDO DE CONFIDENCIALIDADE E SEGURANÇA DA INFORMAÇÃO

IDENTIFICAÇÃO DO CONTRATO

N° do Contrato:	
Empresa Contratada:	
CNPJ:	
Objeto Resumido:	
Vigência Contratual:	

TERMOS

O representante abaixo qualificado do prestador de serviço declara ter pleno conhecimento de suas responsabilidades no que concerne ao sigilo a ser mantido sobre as atividades desenvolvidas ou as ações realizadas no âmbito do Contrato n° 123456, bem como sobre todas as informações que eventualmente ou por força de suas funções venha a tomar conhecimento, comprometendo-se a guardar o sigilo necessário nos termos da legislação vigente e a prestar total obediência às normas de segurança da informação vigentes no ambiente do CONTRATANTE ou que venham a ser implantadas a qualquer tempo por este.

OBSERVAÇÕES

--

DE ACORDO

E, por assim estarem justas e estabelecidas as condições, o presente ACORDO DE CONFIDENCIALIDADE é assinado pelas partes em 02 (duas) vias de igual teor e um só efeito.

Local: _____, Data: ____/____/_____

IDENTIFICAÇÃO E ASSINATURA DO DECLARANTE

Nome: CPF:	Assinatura

IDENTIFICAÇÃO E ASSINATURA DO REPRESENTANTE DO BANCO INDUSCRED

Nome: CPF:	Assinatura

Anexo II. Termo de Ciência da Política de Segurança da Informação

TERMO DE CIÊNCIA DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

IDENTIFICAÇÃO DO COLABORADOR

Nome Completo:	
CPF:	
Função:	

TERMOS

O colaborador acima qualificado declara ter pleno conhecimento de suas responsabilidades no que concerne ao sigilo a ser mantido sobre as atividades desenvolvidas ou as ações realizadas no âmbito dos trabalhos realizados pelo Banco Induscred, seja em suas instalações ou remotamente, bem como sobre todas as informações que eventualmente ou por força de suas funções venha a tomar conhecimento, comprometendo-se a guardar o sigilo necessário nos termos da legislação vigente e a prestar total obediência às normas de segurança da informação vigentes no ambiente do CONTRATANTE ou que venham a ser implantadas a qualquer tempo por este.

OBSERVAÇÕES

--

DE ACORDO

E, por assim estarem justas e estabelecidas as condições, o presente TERMO DE CIÊNCIA é assinado pelas partes em 02 (duas) vias de igual teor e um só efeito.

Local: _____**, Data:** ____**/**____**/**_____

IDENTIFICAÇÃO E ASSINATURA DO DECLARANTE

Nome: CPF:	Assinatura

IDENTIFICAÇÃO E ASSINATURA DO REPRESENTANTE DO BANCO INDUSCRED

Nome: CPF:	Assinatura

Anexo III. Sala dos Servidores e Equipamentos de Rede

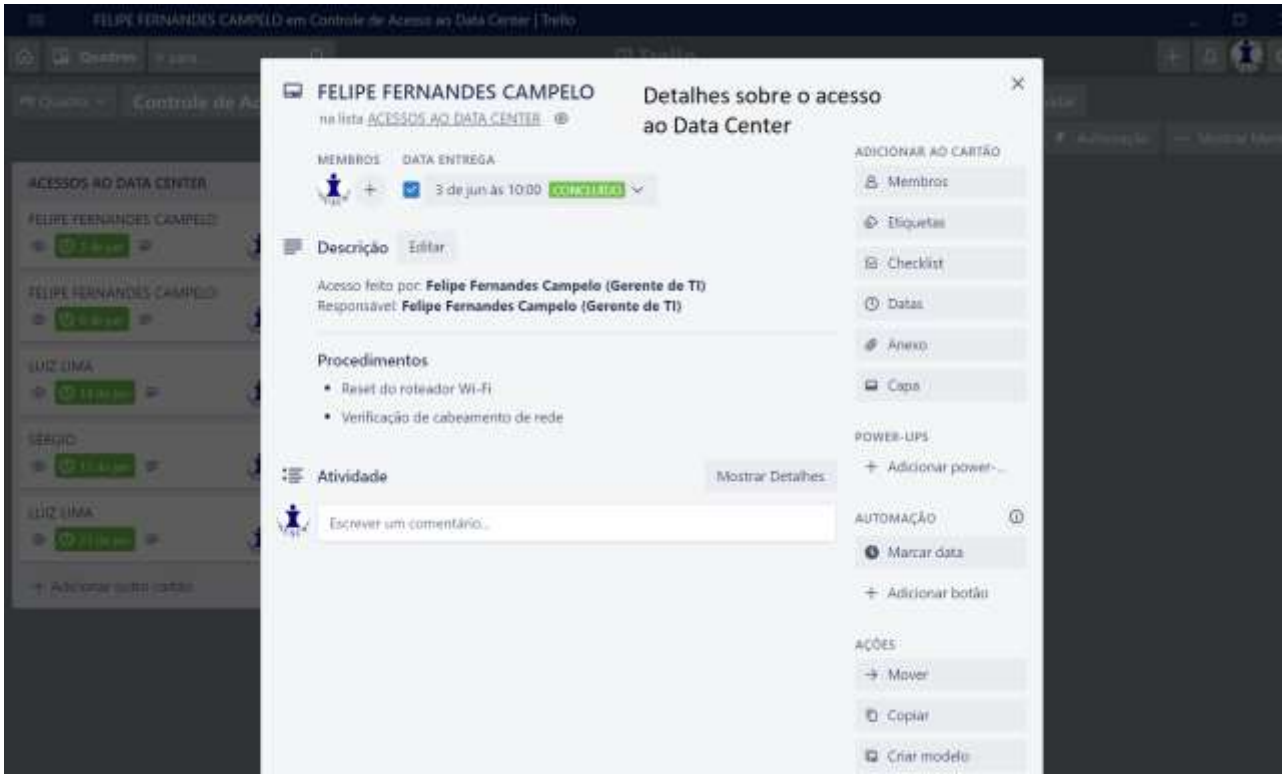
Figura 1 - Ar condicionado da sala dos servidores

Figura 2 - Temperatura padrão da sala dos servidores

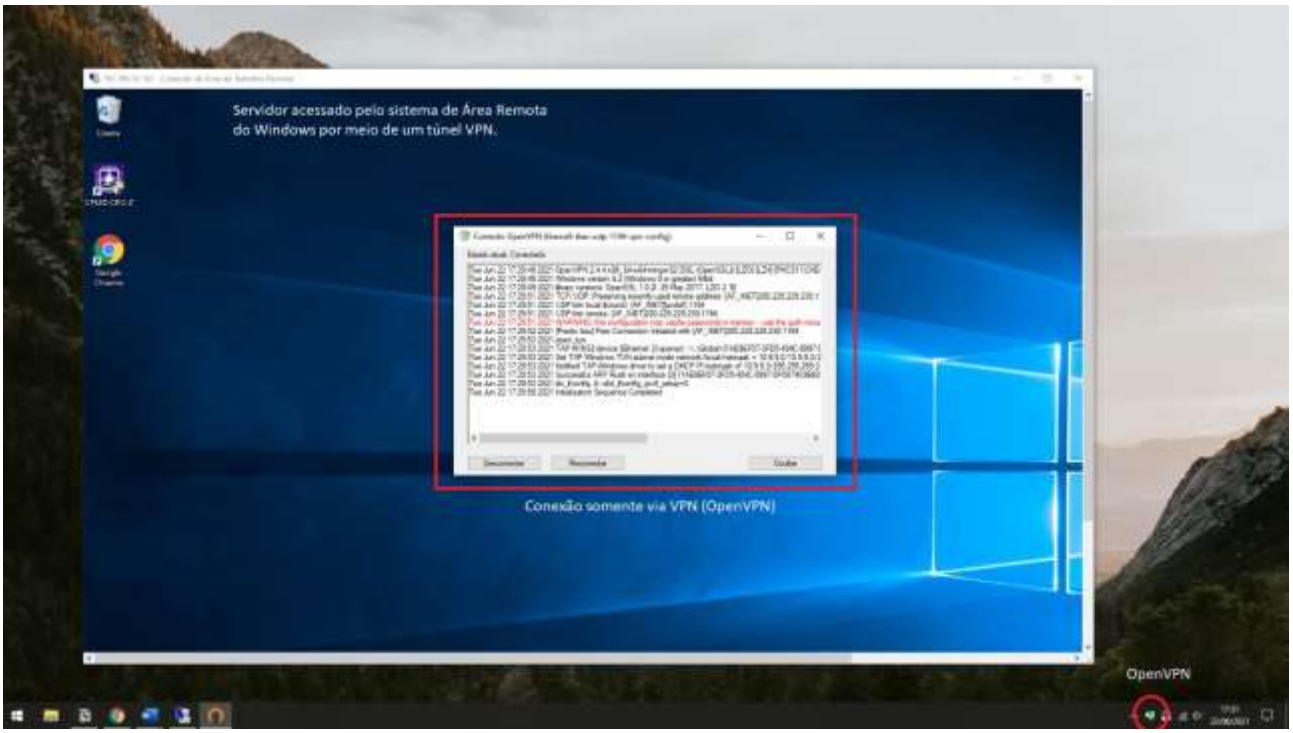
Figura 3 - Armário dos servidores

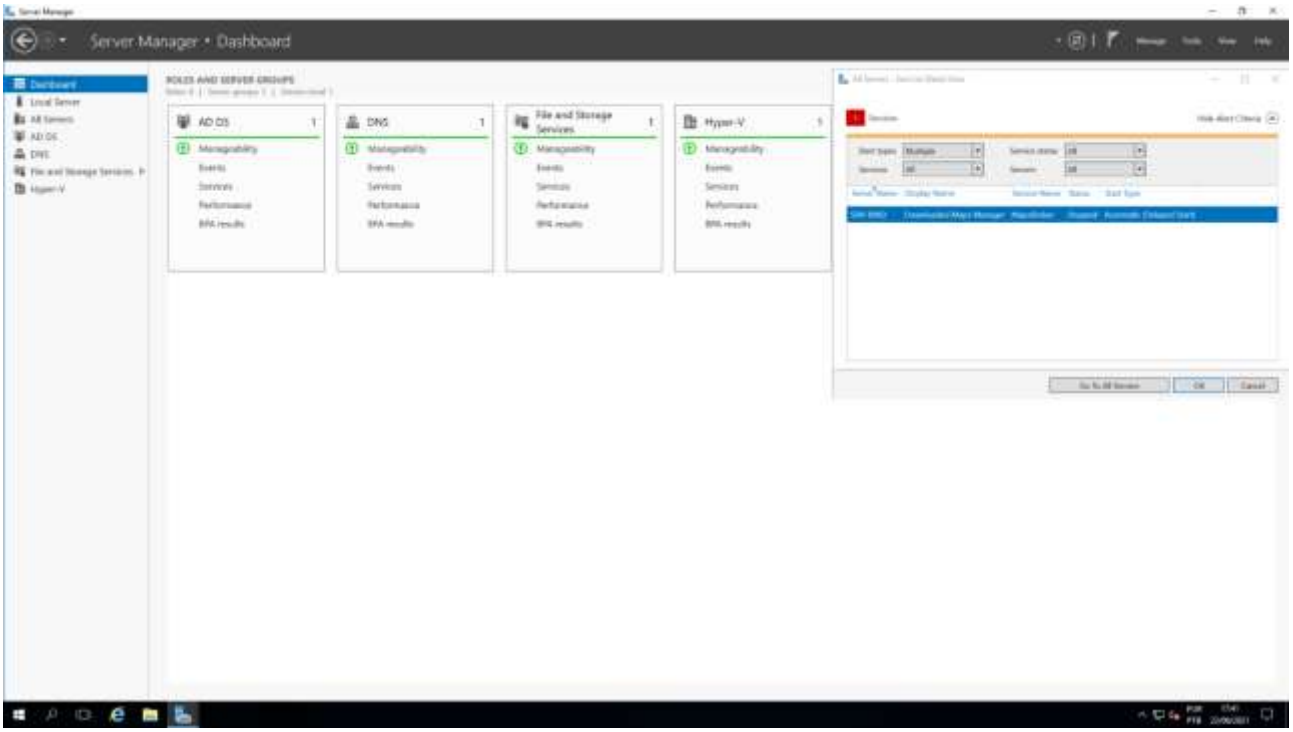
Figura 4 - Armário dos equipamentos de rede

Anexo IV. Registro digital de acesso à sala dos servidores na plataforma Trello

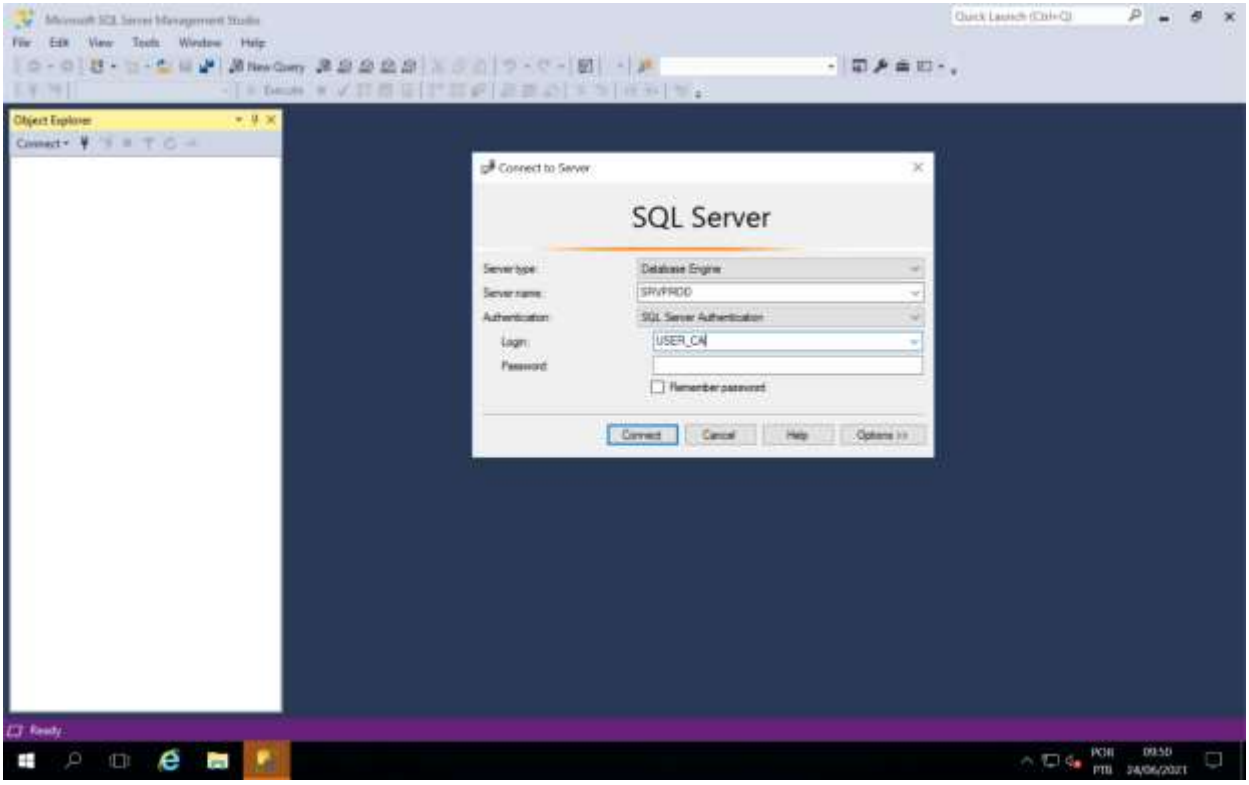


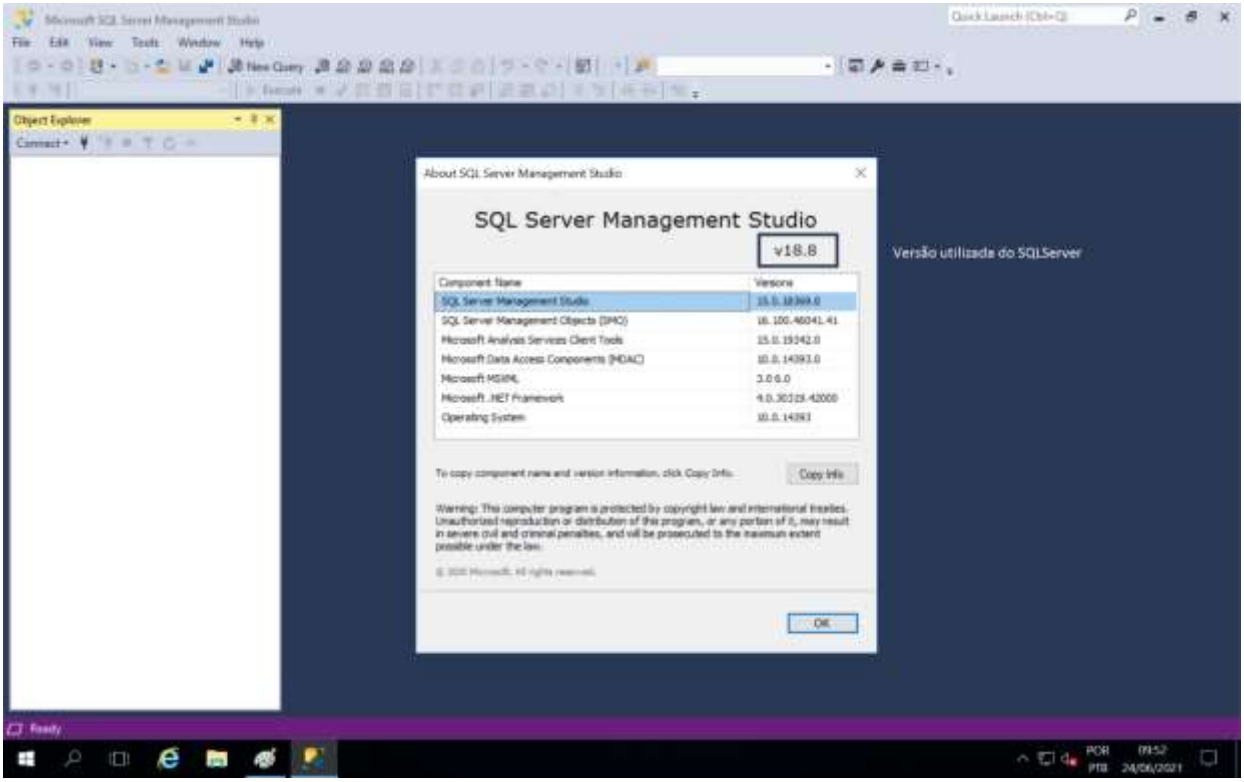
Anexo V. VPN para acesso ao servidor e Máquinas Virtuais





Anexo VI. SQL Server – Banco de dados utilizado pelos sistemas da Autbank





Anexo VII. Registro de scripts a serem executados nos bancos de dados