BANCO RCI BRASIL S.A.

CNPJ Nº 62.307.848/0001-15 - NIRE 41.300.075.336

(Companhia Aberta)

ATA DE REUNIÃO DO CONSELHO DE ADMINISTRAÇÃO

DATA, HORA E LOCAL: 31.03.2023, às 10:30 horas, na sede social do Banco RCI Brasil S.A. ("Companhia"), localizada na Rua Pasteur, 463, 1º andar, conjunto 101, Batel, CEP 80250-080, Curitiba – PR.

PRESENÇA: Presentes os membros do Conselho de Administração da Companhia ao final assinados.

MESA: Sr. Jean-Philippe Jacques Maurice Vallée – Presidente da Mesa; Maick Felisberto Dias – Secretário da Mesa.

ORDEM DO DIA: (i) Deliberar sobre a aprovação da Política de Segurança Cibernética e o Plano de Ação e Resposta a Incidentes Cibernéticos do BANCO RCI BRASIL S.A. ("Companhia"), conforme previsto na Resolução do Conselho Monetário Nacional n.º 4.893/2021 ("Resolução CMN 4.893"); e (ii) Apresentar e conhecer o Relatório anual mencionado pelo art. 8º da Resolução CMN 4.893.

DELIBERAÇÕES: Após exame e discussão da matéria constante da ordem do dia, os membros do Conselho de Administração: (i) deliberaram, por unanimidade de votos dos presentes e sem quaisquer restrições, aprovar a Política de Segurança Cibernética e o Plano de Ação e Resposta a Incidentes Cibernéticos da Companhia, conforme previsto na Resolução CMN 4.893, cujas cópias serão parte integrante desta Ata como Anexos I e II, respectivamente; e (ii) conheceram do Relatório anual mencionado pelo art. 8º da Resolução CMN 4.893referente à data base de 31 de dezembro de 2022.

ENCERRAMENTO: Nada mais havendo a tratar, foi lavrada a presente Ata que foi então lida e achada conforme por todos os presentes que a subscrevem. Mesa: Jean-Philippe Jacques Maurice Vallée - Presidente da Mesa. Maick Felisberto Dias - Secretário da Mesa. Conselheiros: Jean-Marc Marie Bernard Saugier- Presidente do Conselho. Denis Ferro Junior, Cezar Augusto Janikian, Jean-Philippe Jacques Maurice Vallee, José Luis Medina Del Río - Conselheiros Efetivos, e Roberto Alexandre Borges Fischetti – Conselheiro Suplente.

Certifico ser a presente transcrição fiel da Ata lavrada no livro próprio.

JEAN PHILIPPE JACQUES MAURICE VALLEE:24086268892
Assinado de forma digital por JEAN PHILIPPE JACQUES MAURICE VALLEE:24086268892 Dados: 2023.04.11 10:58:42 -03'00'

Jean-Philippe Jacques Maurice Vallée
Presidente da Mesa

MAICK FELISBERTO DIAS
Assinado de forma digital por MAICK FELISBERTO DIAS Dados: 2023.04.11 13:37:08 -03'00'

Maick Felisberto Dias
Secretário da Mesa

* * *

Tipo de Documento:	**Procedimento Local**

Política de Segurança Cibernética

Objeto do documento:	O objetivo desta Política consiste em formalizar as regras, conceitos e Controles de Segurança Cibernética da Mobilize Brasil, com base nas premissas da Política de Segurança da Informação do Grupo Renault, assim como na Resolução nº 4.658, de 26 de abril de 2018 do Banco Central do Brasil e demais normas e disposições aplicáveis. A Diretoria Geral é a área responsável na Mobilize Brasil pelo tema de Segurança Cibernética (e referida política).
Data da aplicação:	09/03/2023
Data da próxima atualização:	09/03/2024
Versão	01/2023
Status:	*Validado*
Departamento:	*Sistemas da Informação*

Autor	**Proprietário do Processo**
Redigido por: Carla Camargo Função: Analista TI SR Data: 09 de março de 2023 | 14:27:02 BRT Assinatura:	Validado por: Isaías Santos Função: Esp. Infraestrutura Data: 12 de março de 2023 | 19:55:46 BRT Assinatura:
Aprovador	**Aprovador**
Aprovado por: Antonio Farias Função: Diretor TI Data: 09 de março de 2023 | 14:35:25 BRT Assinatura:	Aprovado por: Carlos Pizzo Função: Gerente Controle Interno Data: 20 de março de 2023 | 16:28:11 BRT Assinatura:

SUMÁRIO

1 REGRAS GERAIS

A informação é vital para nossa empresa, faz parte de nosso patrimônio e, por essa razão, deve ser protegida.
Enquanto usuários da Informática, temos uma responsabilidade coletiva pela proteção da informação e pela preservação da atividade do Grupo.
A estrutura desta Política de Segurança Cibernética segue os princípios aplicáveis às filiais do grupo Mobilize Banque.

1.1 APLICABILIDADE

Esta política se aplica a todos os usuários da Informática do Grupo Mobilize Brasil, bem como aos prestadores de serviços, estagiários, temporários e fornecedores. Todos estes atores devem conhecer os princípios fundamentais e o comportamento a ser adotado por todos estes atores individualmente para garantir a segurança dos sistemas de informação e a proteção de dados.

2 OBJETIVO E PARTICIPANTES

2.1. OBJETIVO

Os sistemas de informação e as infraestruturas associadas podem ser prejudicados por ameaças de todo tipo em especial má utilização, erro humano, ação mal-intencionada etc.
O objetivo da Política de Segurança dos Sistemas de Informação do Grupo Mobilize Brasil (a seguir chamada Política) é fornecer princípios e regras que permitam proteger nossa atividade contra essas ameaças.

2.2. PARTICIPANTES E SEUS PAPÉIS

COLABORADORES MOBILIZE BRASIL: É fundamental que todos os funcionários conheçam a Política de Segurança da Informação e seus conceitos, para que cada um seja ator consciente da segurança

VOCABULÁRIO E TERMINOLOGIAS:

TERMO	DEFINIÇÃO
CMSSI	Corresponsavel Métier de segurança dos Sistemas de Informação
RMSSI	Responsável Métier de Segurança dos Sistemas de Informação
CSI	Correspondente de Segurança Informática
BCP	Business Continuity Plan
DRP	Disaster Recovery Plan

3 PRINCIPAIS ETAPAS DO PROCESSO

3.1. SÍNTESE DE POLÍTICA DE SEGURANÇA DOS SISTEMAS DE INFORMAÇÃO

A informação é vital para nossa empresa, faz parte de nosso patrimônio e, por essa razão, deve ser protegida. Ela se apresenta sob diferentes formas:

- Programas de financiamento;
- Planos comerciais;
- Dados financeiros;
- Processos de funcionamento ...etc.

Esta informação é ameaçada de diversas maneiras, desde a revelação voluntária ou não de dados sigilosos até a destruição de dados por vírus ou outros.

As consequências dessas ameaças são graves e múltiplas: nossa competitividade, nossa imagem e a confiança de nossos acionistas padecem com elas. Na maioria dos casos, essas situações são evitáveis.

Enquanto usuários dos sistemas de informação, temos uma responsabilidade coletiva pela proteção da informação e pela preservação da atividade de IS/IT do Grupo. Queremos atingir esses objetivos apoiando-nos em três linhas de defesa:

1. **O colaborador** e sua evolução para o comportamento cidadão-empresa, para que cada um seja ator consciente da segurança, através de:
    - Sensibilização para a importância do comportamento dos usuários.
    - Acompanhamento na utilização das ferramentas de segurança.
    - Reforço e animação da rede de correspondentes de segurança presentes em todos os sites da Mobilize Brasil, Renault e seus parceiros.
2. **A área de T.I.**, que proporciona:
    - Ferramentas a serviço dos usuários.
    - Regras técnicas aplicáveis aos Sistemas de informação.
    - Arquiteturas técnicas de segurança.
3. **O controle da conformidade (Realizado pela Matriz)**. Não será detalhado por razões confidenciais e se apoia sobre:

    - Auditorias periódicas de avaliação de nossa resistência aos ataques.
    - Investigações que nos permitem remontar às fontes das falhas.

Todos os colaboradores da Mobilize Brasil devem ler, e aplicar ao cotidiano a Política de Segurança dos Sistemas de Informação, que fornece regras sobre as duas primeiras linhas de defesa.

A Política Geral descreve os fundamentos escolhidos pela empresa, a organização da segurança e as instâncias decisórias.

As Regras de Utilização para todos os colaboradores, da Mobilize Brasil ou não, usuários da Informática. Propondo num grande perfil regras simples, que visam integrar o usuário em nosso sistema de defesa e dar-lhe os meios de atingir o comportamento cidadão-empresa.

As Regras de Implementação Técnica destinadas a equipe de T.I. responsável pela implementação dos meios técnicos. Elas definem com precisão as soluções técnicas escolhidas e permitem empregar na prática, hoje, as defesas de amanhã.

3.2. DEFINIÇÕES DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

O ambiente global

O ambiente global dentro do qual evolui a empresa esconde oportunidades que, se não se tomar cuidado, podem ocultar grandes ameaças. Este documento Política de Segurança visa fornecer diretrizes para melhor se proteger contra esses perigos ocultos.

Neste contexto define, dentro do ambiente empresarial global, os principais pontos de exposição da segurança da informação:

Os colaboradores: inconsequência e má intenção

Os riscos podem proceder:

- Da utilização abusiva dos meios de Informática. Diante disso, somente uma ação sobre nossos comportamentos através da sensibilização e através da revisão da Termo de Responsabilidade e Compromisso permitirá prevenir eficazmente.
- Ataques implementados por pessoas isoladas, grupos ideológicos, organizações criminosas e mesmo órgãos de espionagem.

O posto de trabalho: janela para o mundo e detentor de dados

O posto de trabalho (PC, telefone, PDA, etc.) está exposto a diferentes riscos tais como furto ou roubo do dispositivo físico, roubo de informações nele contidas que incluem diferentes tipos de documentos inclusive lista de contatos, agendas, etc, podendo, além disto:

- Funcionar como ponte para uma intrusão à distância na rede do Grupo.
- Causar perturbação à produtividade do usuário enquanto espera a substituição do dispositivo ou resolução do incidente de segurança.
- Perda econômica para o Grupo decorrente da perda do próprio dispositivo ou de informações necessárias para o negócio do Grupo, nele contidas.
- Propagador de vírus, de malware.

Internet: revolução dos modos de intercambio

A utilização da Internet apresenta vantagens, mas também riscos:

- **A navegação web** expõe o ambiente a programas mal-intencionados que permitem a tomada de controle à distância, o download remoto de arquivos infectados ou de códigos maliciosos, o registro de toques do teclado.
- **As trocas de arquivos** nas redes « peer-to-peer » ou nas plataformas de transferência de arquivos, são capazes de introduzir programas espiões e códigos maliciosos no PC, e mesmo permitir vazamento de informação.
- **As mensagens instantâneas** podem ser utilizadas para enviar/receber dados confidenciais não criptografados e arquivos com documentos anexos, potencialmente infectados, burlando, entre outros, os sistemas antivírus do Grupo, implementados pelo correio eletrônico.
- **O correio eletrônico**. Além do documento anexo que pode estar infectado, certos ataques têm por alvo os pontos fracos dos clientes de e-mail.
- **As redes sociais** nas quais as pessoas dão informações inocentemente ou como promoção pessoal sem medir a exposição aos perigos tais como a informação para a concorrência, a fonte de intrusões posteriores.

As leis: endurecimento e globalização

O crescimento do Grupo Mobilize deve respeitar as barreiras impostas pelas leis e regulamentações locais com as quais os processos ofícios e os sistemas de informação devem guardar conformidade. Os aspectos legislativos nacionais e internacionais têm um peso importante na concepção dos sistemas de informação.

Os sistemas de informação: abertura e exposição

Nosso patrimônio de aplicativos, programas e dados, estão expostos aos seguintes riscos:

- À abertura dos sistemas de informação aos parceiros externos;
- Ao acesso dos usuários internos;
- Ao uso dos sistemas de informação externos.

Em síntese:

Sem que estejamos conscientes do risco inerente ao uso dos sistemas de informação, nossas ações podem estar na origem da ativação de ameaças aos sistemas de informação e diretamente aos dados, maior patrimônio do Banco.

O impacto destas ameaças sobre nossa atividade foi medido em termos de dois riscos importantes:

- A interrupção da atividade de Informática e consequente parada do negócio.

- O roubo ou a falsificação de dados confidenciais e consequentes impactos legais e financeiros para a Empresa.

Nossa resposta:

Devemos enfrentar essas diferentes ameaças com dois objetivos maiores:

1. A preservação da atividade de Informática.
2. A proteção da informação.

Para isso, construímos três linhas de defesa:

O colaborador, isto é, o usuário e seu comportamento como "cidadão-empresa". Devem todos ser atores conscientes da segurança, atentos:

- Ao nível de sensibilidade da informação, aos comportamentos a ter e às precauções a aplicar ao manipular informações, o que se buscará pela:
    - Promoção dos módulos de treinamento de segurança da informação (e-learning ou presencial), simulações das situações de risco e apresentação/atualização das regras de utilização dos sistemas de informação e de segurança de dados.
    - Organização de sessões (reuniões, e-mails orientativos) de sensibilização sobre respeito à Política de Segurança.
    - Engajamento da alta Administração na aplicação da Política.
- A extensão e a animação da rede de correspondentes de segurança.
    - Identificação de correspondentes de segurança Mobilize
    - Comunicação sobre acontecimentos com impacto sobre a segurança e suas consequências.
    - Animação em torno de indicadores para acompanhar os planos de ação.

A Área de T.I.: Como fornecedora de novas funcionalidades para os usuários, para o negócio e também para os chefes de projeto de Informática e desenvolvedores. Deve atender a estas necessidades com recursos que representem o “estado da arte” mas que respeitem as regras de segurança para infraestrutura e desenvolvimento seguros adotada pelo Grupo de maneira a evitar a exposição dos sistemas de informação a riscos desnecessários, considerando minimamente, mas não se restringindo a:

- A identificação forte dos usuários e rastreamento especialmente para as conexões remotas, etc.
- A criptografia dos dados por ocasião de seu armazenamento nos postos de trabalho (PC, token USB, etc.), nos servidores e por ocasião do transporte deles dentro e fora da rede.
- A segregação de certas partes da rede para um melhor controle interno.
- Soluções técnicas de segurança a serem integradas já na fase de concepção dos projetos.
- Soluções técnicas para proteção dos ativos como antivírus, aplicação automatizada de patches de correção de vulnerabilidades de sistema operacional com atualizações automáticas e periódicas.
- Definição das regras para desenvolvimento seguro de softwares.
- Definição de regras para a criação segura de arquitetura de softwares.
- Proteção e controle de acesso aos dispositivos de rede, servidores e postos de trabalho.
- Definição dos padrões seguros para conectividade ponto-a-ponto com fornecedores externos.
- Definir as regras de utilização de ativos de TI.
- Validação da capacidade técnica e definição dos níveis de acesso para prestadores de serviços em TI.
- Apresentação de mudanças no ambiente produtivo de acordo com o processo de Gestão de Mudança do Grupo.
- O engajamento da Direção para provimento dos recursos necessários para a implementação das soluções técnicas de segurança, necessárias para a proteção dos sistemas de informação.

Todo acesso aos documentos relativos às definições e regras é restrito e está sujeito à controle pela área responsável.

O controle da conformidade. Equipe encarregada da realização dos planejamentos e acompanhamento das execuções programadas dos testes de intrusão e do plano de comunicação e recuperação de incidentes cibernéticos. Realiza a síntese das execuções em forma de indicadores a serem criados de acordo com a definição da Direção de TI.

3.3. OS PRINCÍPIOS FUNDAMENTAIS DA POLÍTICA

A segurança dos Sistemas de Informação do Grupo repousa sobre os seguintes princípios fundamentais:

1. **Cada usuário** age enquanto cidadão-empresa
   A proteção dos recursos e dados da empresa repousa em grande parte no "civismo" de todos. Este comportamento qualificado de « cidadão-empresa » se adquire pelo conhecimento e pela aplicação no dia a dia de um conjunto de regulamentos, de políticas e de orientações definidos no interior do Grupo, e é descrito através de regras de utilização. Cada usuário deve estar consciente de sua responsabilidade, agir como ator engajado e vigilante da segurança, sabendo que seus acessos são rastreados.

2. **Todo usuário de recursos de Informática deve ser identificado.**
   - O usuário pode ser um indivíduo, um aplicativo, e existem vários tipos de identificação (empregados, fornecedores, prestadores de serviço, virtuais, técnicos, etc.).
   - A identificação permite atribuir os direitos de acesso à rede e aos sistemas de informação.
   - Esta identificação pode ser associada a mecanismos de autenticação que certificam a identidade.

3. **A homologação do posto de trabalho é obrigatória**.
   - A homologação garante:
     - Uma configuração mínima de segurança e sua atualização diante da evolução permanente das ameaças (antivírus, patch de OS.).
     - A existência de um suporte através da função assistência ao posto de trabalho no caso de incidente ou de ataque de Informática.
   - O posto de trabalho homologado evita uma disseminação de dados potencialmente confidenciais sobre equipamentos não controlados.

4. **Toda a conexão na rede de Informática deve ser estritamente validada.**
   A rede de Informática Mobilize, também chamada Intranet, é uma zona de segurança que facilita os intercâmbios entre os sites do Banco. É preciso proteger suas fronteiras aplicando as diretrizes seguintes:
   - Toda e qualquer conexão entre a Intranet e um terceiro, não validada pela Direção de T.I, é proibida.
   - Toda conexão de um equipamento não homologado Mobilize na Intranet está proibida.
   - Os acessos à Intranet a partir de fora se fazem através dos meios centrais e estão sujeitos à autenticação.

5. **Os aplicativos e os dados devem ser protegidos em função de seu caráter crítico.**
   - Todo sistema de informação deve ser estruturado para ser acessível de maneira segura por usuários não-Mobilize a partir da Intranet do Banco ou das Extranets homologadas (parceiros, fornecedores, etc.). Isto implica em particular uma gestão adaptada das identidades e direitos de acesso de aplicativos.
   - Todo sistema de informação que controla dados da Mobilize deve, segundo seu nível de classificação de segurança, conservar o rastreamento pista dos acessos e das operações que lhe são pedidas (quem, o quê, quando) e se o caráter confidencial é considerado crítico ou estratégico, deve ser instalado em uma zona-rede protegida (DMZ) no interior da Intranet do Grupo.
   - O desenvolvimento internacional dos aplicativos com os Métiers deve-se fazer dentro do respeito às leis e aos regulamentos nacionais aplicáveis aos dados controlados.
   - Procedimentos de recuperação no caso de incidente são redigidos e periodicamente testados.

3.4. ORGANIZAÇÃO DA GESTÃO DA SEGURANÇA DOS SISTEMAS DE INFORMAÇÃO

A Política é definida em função dos riscos e limitações identificados pelas diferentes Direções Métiers do Banco e a Direção dos Sistemas de Informação Mobilize e leva em consideração os princípios fundamentais lembrados anteriormente. Ela propõe regras de utilização para agir sobre o comportamento e regras de implementação técnica para padronizar e expandir o portfólio das ferramentas técnicas a fim de atingir seus objetivos de continuidade da atividade de Informática, assim como de sigilo e integridade dos dados.

O desenvolvimento dessas regras é pilotado pela Direção dos Sistemas de Informação Mobilize através das instâncias de pilotagem de Informática (Comitês).

Para definição e acompanhamento da aplicação das regras de segurança dos sistemas de informação, a Política define uma organização-tipo desenvolvida ao mesmo tempo pela Informática e pelos Métiers da áreas:

1. Direção dos Sistemas de Informação Mobilize, responsável por:
    - RSSI: Responsável Loca de Segurança da Informação, que tem como responsabilidades:
        - Definir a política local e fazer aplicar as normas de segurança do Corporate;
    - Correspondentes Segurança Informática (CSI), que garante o suporte de campo e a aplicação da Política.
2. Cada Direção Métier usuária dos Sistemas de Informação
    - O responsável Métier pela Segurança dos Sistemas de Informação (CMSSI), explica e faz aplicar a Política no interior do seu Métier.
    - Correspondente Métier de Segurança da Informação: dirigem no dia a dia as ações para a manutenção e respeito da Política em cada área metier.

4 IMPLEMENTAÇÃO DA POLÍTICA DE SEGURANÇA DOS SISTEMAS DE INFORMAÇÃO

4.1 REGRAS DE UTILIZAÇÃO DOS RECURSOS DE INFORMÁTICA

a) Para qualquer usuário no uso do posto de trabalho padrão:

Todo colaborador Mobilize deve conhecer e aplicar as regras e precauções abaixo:

1. Utilizar seu identificador (IPN) associado a uma senha pessoal, forte, modificada regularmente e conservada estritamente confidencial. Jamais utilizar o identificador de uma outra pessoa.
2. Utilizar os meios de informática do Grupo no âmbito de sua atividade profissional e não instalar ou mandar instalar programas ou hardwares que não sejam aqueles fornecidos pelo Grupo Mobilize Brasil.
3. Utilizar seu posto de trabalho em conformidade com o Termo de Responsabilidade e Compromisso
4. Proteger seu posto de trabalho, PC fixo ou portátil, assistente pessoal, telefone, etc.:
    - Contra o roubo.
    - Contra o uso ilícito de sua sessão de trabalho.
5. Proteger a confidencialidade das informações estratégicas e críticas presentes nos PCs e nas mídias removíveis, ou e-mails.
6. Abolir todo relacionamento da rede Mobilize com uma rede de terceiros por intermédio de algum equipamento ou método, qualquer que seja.
7. Proibir-se de retransmitir os e-mails inoportunos, perigosos ou ilícitos, e não abrir e-mails desconhecidos nem documentos anexos suspeitos (arquivos executáveis, publicidade, etc.).
8. Proibir-se de comunicar informação referente ao Grupo ou sua atividade profissional sem validação prévia pelo superior hierárquico e a Direção de Recursos Humanos.
9. Proibir-se a utilização de e-mails de domínio público para necessidades profissionais e só utilizar o correio eletrônico Mobilize

10. Verificar se um acordo de confidencialidade Mobilize foi assinado por todas as pessoas com acesso a dados confidenciais.
11. Ficar vigilante e alertar seu superior no caso de anomalia suspeita.

b) Para qualquer usuário no uso da Internet:

Além das regras e precauções descritas acima, toda e qualquer utilização da Internet deve:

1. Utilizar a Internet em conformidade com o Termo de Responsabilidade e Compromisso.
2. Utilizar identificadores e senhas diferentes daqueles empregados no interior da empresa para os acessos às suas contas nos sites Internet. Preferir identificadores diferentes se você estiver em vários sites.
3. Verificar os parâmetros default de sua conta em cada site Internet para certificar-se de que seus dados não sejam visíveis a todos e minimizar as informações pessoais que você divulga.
4. Evitar pôr online fotos, vídeos embaraçadores ou comprometedores, que possam prejudicá-lo assim como a seus próximos, à sua empresa ou a seus clientes.
5. Não utilizar os sites de mídias sociais como diário íntimo, salvo se você tiver certeza de que todos, famílias, amigos, inimigos, superiores hierárquicos, etc. conhecem tudo a seu respeito.
6. Autocontrolar-se nos blogs, fóruns, chats para não se deixar levar a provar seu ponto de vista dando informações, indicações prejudiciais à sua vida privada ou à sua empresa.
7. Proibir-se, fora da necessidade profissional, de baixar vídeos, imagens, de ver TV ou escutar rádio, pois isto provoca um afluxo de dados capaz de degradar os desempenhos de acesso de seus colegas aos aplicativos Métiers da Empresa.
8. Conhecer o expedidor não justifica clicar sobre os links do e-mail recebido. Se o e-mail lhe parece suspeito, é porque ele provavelmente é.
9. Desconfiar dos spams que tentam obter dados enviando convites não solicitados. Ignorar toda solicitação se você não conhecer a pessoa.
10. Ficar fora de perigo utilizando somente computadores que tenham um programa antivírus atualizado, um firewall ativado e um bom nível de patches.

c) Para o prestador de serviços no local

Todo prestador de serviços tem a responsabilidade de aplicar as regras e precauções próprias ao usuário Mobilize:

- Seus acessos lógicos devem ser validados pelo menos uma vez por ano
- Seu perfil de acesso ARCA deve ser mantido em dia.

d) Para o visitante

O visitante não está autorizado a conectar-se com a Intranet Mobilize. Se ele tiver necessidade de uma conexão externa, deverá fazê-lo pela conexão WiFi Hot Spot que fornece, apóss a autorização pela Mobilize, um acesso limitado e controlado a um certo número de sites da Internet.

e) Para os novos Colaboradores

Novos colaboradores devem receber o Termo de Responsabilidade e Compromisso no momento da contratação, com assinatura, a mesma encontra-se no kit de contratação.

Adicionalmente, no processo de Integração de novos colaboradores será realizada a apresentação da Política de Segurança de Informação pela área de T.I.

4.2 MAPEAMENTO DE DADOS

Para classificação dessas bases de dados, foram aplicados os seguintes critérios de classificação:

	Classificação da Informação			
	Nível 1 – INTERNAL	**Nível 2CONFIDENTIAL**	**Nível 3 – RESTRICT B**	**Nível 4 – SECRET A**
CONCEITO	Acesso livre para qualquer pessoa com status de residente na Mobilize ou acessando a intranet Declic do grupo Renault. No entanto a informação permanece propriedade da Mobilize e não deve ser comunicada fora do grupo, salvo menção específica.	Acesso restrito a um grupo limitado (direção, métier, projeto	Acesso restrito individual e nominativo às pessoas que tenham estrita necessidade de utilizar a informação. Os destinatários podem copiar ou retransmitir a informação com o acordo de sua hierarquia. Os fluxos de intercâmbio de informações devem ser protegidos.	Acesso restrito a um pequeno número de pessoas habilitadas. As pessoas autorizadas são alertadas de sua responsabilidade e se comprometem com a confidencialidade. Os meios de informação são sistematicamente protegidos. A retransmissão da informação está submetida à decisão da entidade proprietária.
EXEMPLO	Informações divulgadas no Declic (intranet do grupo)	Atas de Reunião; Apresentações da Equipe, Procedimentos	Modelos de Negócio ,Relatório de Fraude Notas de Comex Bonificação da Rede Concessionário .	Projetos Estratégicos; Dados Financeiros antes da Publicação

5 GOVERNANÇA DOS INCIDENTES CIBERNETICOS

A segurança cibernética tem como fundamento oferecer à Organização:

- A capacidade de identificar, detectar e proteger-se, em todo espaço cibernético, contra cyber ataques que possam gerar um incidente de segurança cibernética
- A capacidade de responder e recuperar-se de forma rápida de uma ameaça que coloque em risco segurança cibernética, afetando a confidencialidade, disponibilidade e integridade dos ativos tecnológicos e informações.

Algumas definições:

- **Espaço cibernético:** engloba a internet, os sistemas de informação, os dispositivos móveis e as tecnologias digitais que dão suporte aos negócios, a infraestrutura e os serviços;
- **Incidente de segurança cibernética:** todo e qualquer evento não esperado que gere algum tipo de instabilidade, quebra de política ou que possa causar danos ao Grupo Mobilize Brasil;
- **Ataque cibernético:** é a exploração por parte de um agente malicioso para tirar proveito de ponto(s) fraco(s) com a intenção de alcançar um impacto negativo no alvo. Os atacantes podem ter como alvo os clientes, fornecedores e parceiros do Santander Brasil para causar impacto significante para a Organização;
- **Risco à segurança cibernética:** advêm de dentro e de fora da Organização. O impacto do risco à segurança cibernética engloba perda financeira, danos à reputação, multas regulatórias, perda de vantagem estratégica e interrupção de operações;
- **Ativos tecnológicos:** é qualquer dispositivo físico ou digital, equipamento ou outro componente do ambiente que suporte atividades relacionadas à informação;
- **Threat intelligence:** consiste em todo conhecimento baseado em evidências, contexto, mecanismos e indicadores sobre ameaças existentes, correlacionando com os ativos tecnológicos que podem ser comprometidos a partir da exploração e concretização dessa ameaça.

Para garantir a eficácia da segurança cibernética é necessária a implementação de procedimentos de governança que definam os atores, as responsabilidades e a categorização dos incidentes para informação e tratamento.

5.1 RESPONSABILIDADES

5.1.1 5.1.1. SOC – SECURITY OPERATION CENTER – CENTRO DE OPERAÇÕES EM SEGURANÇA:

Responsável pela detecção e análise dos incidentes cibernéticos que possam impactar os sistemas de informação e a confidencialidade dos dados. Todos os analistas do SOC devem conhecer e respeitar as normas do código de ética do Grupo.
O SOC deve garantir a traçabilidade do incidente cibernético até seu encerramento completo.
Na região do Brasil a Mobilize não possui um SOC dedicado e, a exemplo das demais subsidiárias Mobilize, utiliza o SOC compartilhado com a Mobilize Central.

5.1.2 5.1.2. CSI: CORRESPONDENTE DE SEGURANÇA DA INFORMAÇÃO:

Principal ponto de contato do SOC e do responsável de segurança do Corporate com a região/país onde atuam. Desta forma devem:
- Reportar para o SOC qualquer incidente ou suspeita de incidentes (ex: malware, cyber ataques);
- Implementar os planos de ação e de contorno definidos pelo SOC;
- Contribuir com o aprimoramento da base de conhecimento do SOC fornecendo todas as informações necessárias para entendimento do contexto do incidente (rede, inventário de ativos, etc.)

Na estrutura da Mobilize Brasil o CSI é membro da equipe de Informática.

5.1.3 5.1.3. GERENTES DE PROJETO E ADMINISTRADORES DE REDE:

Devem colaborar com o CSI na análise dos incidentes cibernéticos e aplicar as ações de contorno e do plano de ações definidas pelo SOC.
Todos os operadores e administradores de rede devem implementar e armazenar logs dos ambientes, respeitando a regulamentação local aplicável e os requerimentos de segurança do Corporate.

5.1.4 5.1.4. USUÁRIOS INTERNOS E EXTERNOS

Assim como qualquer ator que utilize sistemas de TI e serviços do Banco: Devem notificar e reportar para o SOC, imediatamente, qualquer vulnerabilidade nos sistemas ou serviços utilizados. Devem ainda encaminhar quaisquer e-mails suspeitos para análise e tratamento pelo SOC.

5.2. POTENCIAIS SITUAÇÕES DE INCIDENTES DE SEGURANÇA

Algumas situações e eventos que constituem potenciais incidentes de segurança notificáveis, não se limitando a elas, são descritas abaixo:

- Checagens de segurança ineficientes
- Violação das precauções de segurança física
- Desvios das condições/regras de segurança definidas
- Violação da integridade, confidencialidade e disponibilidade:
    - Tentativas bem-sucedidas de acesso não autorizado às informações;
    - Uso, publicação, modificação ou destruição não autorização de informações;
    - Interrupção frequente dos sistemas de informação
    - Acesso não autorizado a sistemas de informação ou às áreas (perfis) nos sistemas de informação
- Desrespeito deliberado das diretrizes e instruções de trabalho da segurança da informação.
- Violação negligente das diretrizes e instruções de trabalho da segurança da informação;
- Propagação deliberada de informação falsa;
- Falta ou insuficiência de regulação de segurança
- Aceitação insuficiente das políticas de segurança da informação
- Abuso de direitos do usuário ou de direitos de administrador;
- Modificações irregulares nos sistemas de informação (incluindo sistemas operacionais e aplicações)
- Anomalias e mal funcionamento de hardware e software (incluindo suspeita de malwares)
- Uso não apropriado de senhas e outros direitos de acesso
- Repetidas tentativas de acesso com senha inválida
- Administração de direitos de acesso e autorização de acesso ineficientes

- Incorreções na configuração de sistema operacional, web server, servidor de aplicação, gerenciamento de banco de dados
- Exploração de vulnerabilidades especificas em sistemas operacionais e aplicações
- Qualquer tipo de malwares (vírus, cavalos de tróia, keyloggers, etc..)
- Qualquer sinal de processos suspeitos ou funcionamento irregular do posto de trabalho
- Roubo de identidade
- Roubo de equipamentos ou vandalismo
- Qualquer perda de mídia de dados (tokens, usb, laptops, etc.)
- Perda de crachás ou qualquer tipo de identificação eletrônica do colaborador.

Além destes eventos, as informações divulgadas pelos meios de comunicação confiáveis, que digam respeito à vulnerabilidade ou exploração de vulnerabilidades são também notificáveis para evitar incidentes cibernéticos. Estas notícias não contam como incidentes de segurança dentro da Organização.

5.3 AVALIAÇÃO E RESPOSTA A INCIDENTES CIBERNÉTICOS

O SOC em conjunto com o CSI deve analisar os eventos reportados pelos diferentes atores para decidir se eles devem ser classificados como incidentes de segurança da informação ou não e avaliar a o nível de criticidade.

5.3.1 5.3.1. DEFINIÇÃO DA CRITICIDADE DOS INCIDENTES DE SEGURANÇA

O critério de avaliação do nível de criticidade deve ser estabelecido de acordo com o nível de exposição dos dados e pelo impacto para a continuidade do negócio do Grupo Mobilize Brasil e, dependendo da classificação, medidas devem ser tomadas considerando o tempo de reação e solução.
A primeira comunicação deve ser feita diretamente ao SOC por meio de correio eletrônico ou outro meio de contato ágil, que garanta que a informação chegue ao responsável de segurança Corporate. Toda a informação necessária para a análise (logs, RCA e outras informações adicionais) deve ser repassada na comunicação do evento. Deve-se levar em conta que como se trata de informação confidencial esta informação precisa ser protegida contra acesso não autorizado e disponibilizada apenas para o grupo de pessoas que necessitam destas informações.

5.3.2 5.3.2. OPERAÇÃO NO TRATAMENTO DE INCIDENTES REPORTADOS

Após receber do CSI a informação de um evento o SOC, o Responsável de Segurança local ou um de seus delegados, são responsáveis pela imediata avaliação de quando o evento começou e fazer a operação/tratamento de acordo com os tempos de reatividades definidos de acordo com a criticidade do incidente.
Os critérios de avaliação formal da criticidade de um incidente bem como a classificação de um evento como incidente de segurança, são definidos pelo Security Officer e devem contemplar avaliação dos itens abaixo, não se limitando a eles:

- As pessoas (físicas ou jurídicas) pode acessar dados (ler/escrever) de clientes em produção sem autorização?
- É possível acessar informações internas/confidenciais/estratégicas sem autorização?
- As pessoas acessaram informações internas/confidenciais/estratégicas sem autorização?
- Dados produtivos de um cliente (informações internas/confidenciais/estratégicas) ou equipamentos (laptops, smartphones, pen-drives, disco externo) foram roubados ou há suspeita de que tenham sido?
- Dados produtivos de um cliente ou informações internas/confidenciais foram publicados de alguma forma (sites externos, e-mails, etc)?
- As diretrizes de segurança da informação, definidas na Política de Segurança, foram deliberadamente desrespeitadas?
- O mesmo evento ocorreu diversas vezes em um período curto de tempo?
- Qual o número de usuários afetados?
- Quanto tempo o evento/incidente durou?
- Dados sensíveis de clientes (dados pessoais) foram afetados? Se sim considerar envolver o DPO.

Com base nesta avaliação será definido o nível de criticidade do incidente e o tipo de comunicação a ser realizada.

5.3.3 5.3.3. NÍVEIS DE CRITICIDADE E COMUNICAÇÃO DOS INCIDENTES DE SEGURANÇA

Os níveis de criticidade dos incidentes são: Critico, Alto, Médio e Baixo. A classificação é realizada com base nos critérios exemplificativos listados acima e pelos demais critérios definidos pelo responsável de segurança.

A comunicação de um incidente é afetada pela classificação dada ao evento, englobando pelo menos o listado no quadro abaixo, sem se limitar a ele.

Criticidade	Comunicação
Crítico	Informação aos Órgãos Reguladores (Banco Central e ANPD): Obrigação legal Por estipulação contratual Violação da privacidade dos dados Informação aos Clientes Violação da privacidade dos dados Informação ao DPO e aos órgãos Reguladores Violação da privacidade dos dados Escalada interna para o Diretor responsável Informação interna para os usuários depois de finalizado o incidente bem como Aplicação do treinamento de Segurança da Informação
Alto	Informação aos Órgãos Reguladores (Banco Central e ANPD): Obrigação legal Por estipulação contratual Violação da privacidade dos dados Escalada interna para o Diretor responsável
Médio	Informação aos Órgãos Reguladores (Banco Central e ANPD): Obrigação legal Por estipulação contratual Violação da privacidade dos dados Escalada interna para o Diretor responsável Informação interna para os usuários depois de finalizado o incidente bem como Aplicação do treinamento de Segurança da Informação
Baixo	Escalada interna para o Diretor responsável Informação interna para os usuários depois de finalizado o incidente bem como Aplicação do treinamento de Segurança da Informação

5.3.4 RESPOSTAS DO SOC SOBRE OS EVENTOS SE SEGURANÇA

Dependendo da natureza do incidente cibernético SOC deve dar a resposta apropriada:

- Definindo e implementando o plano de ação para resolver ou minimizar os riscos;
- Disponibilizando os diferentes atores que que atuarão nas diferentes frentes de solução;
- Acompanhando e checando a implementação dos planos de ação até que estejam formalmente finalizados;
- Definindo o plano de comunicação apropriado.

- Realizando ou acompanhando a realização da comunicação aos órgãos Regulatórios.
- Realizando nova análise do cyber incidente depois de encerrado quando a situação exigir.

O SOC, CSI, RMSI e o Diretor de TI local devem implementar meios (base de conhecimento) que permitam prevenir ou reduzir impactos e a probabilidade de ocorrência de incidentes similares.

6 REGRAS DE CONTROLE DA APLICAÇÃO DO PROCESSO

6.1 CONTROLES DE PRIMEIRO NÍVEL:

6.1.1 CONTROLE DE PRIMEIRO NÍVEL KPI 21 IT SECURITY

Controle formalizado no Procedimento DRP Mobilize.

7 INDICADORES DE ACOMPANHAMENTO

O acompanhamento é realizado pelo indicador comum do Grupo classificado como KPI 21 – Segurança da Informação, checado de forma mensal.
Havendo não-conformidades o indicador é impactado e um plano de ação é aberto. A definição do plano de ação fica à cargo do Diretor TI local e a implementação das ações definidas é acompanhada pelo time de Controle Interno.

8 CONTROLE DE ALTERAÇÕES

Versão	Autor	Proprietário do Processo	Principais Mudanças
01/2022	Isaias Santos	Antonio Farias	1. Revisão Geral do Processo 2. Atualização da Aplicabilidade para o Grupo RCI Brasil.
01/2023	Isaias Santos / Carla Camargo	Antonio Farias	Ajustada a tabela de níveis de confidencialidade PMI

RELATÓRIO ANUAL – RESOLUÇÃO 4658

REFERÊNCIA - 2022

SEGURANÇA DA INFORMAÇÃO
MOBILIZE BRASIL
Rua Pasteur, 463 Curitiba-PR-Brasil

Sumário

Autor	Responsável	Aprovador
Redigido por: Isaias Santos / Carla Camargo Função: Coordenador TI / Analista Infra Data: Assinatura:	Validado por: Isaias Santos Função: Coordenador TI Data: Assinatura:	Aprovado por: Antonio FARIAS Função: Diretor TI Mobilize Brasil Data: Assinatura:

Aprovador	Aprovador
Aprovado por: Carlos PIZZO Função: Gerente Controle Interno Data: Assinatura:	Aprovado por: José Medina Função: Diretor Geral Mobilize Brasil Data: Assinatura:

1. VISÃO GERAL

A informação é considerada um dos principais patrimônios das organizações, sendo assim a adoção de estruturas que visam garantir a segurança, preservação da integridade e disponibilidade destas informações são de suma importância para garantir os o exercício dos direitos do titular e para direcionar esforços para reduzir as ameaças. Para o Banco Mobilize as informações são vitais, fazem parte de nossos ativos e, por isso, devem ser devidamente protegidas.

A Resolução n° 4.658 de 26 de abril de 2018 publicada pelo Banco Central do Brasil determina em seu Art. 8º que seja elaborado relatório anual sobre a implementação do plano de ação e de resposta a incidentes (data base de 31 de dezembro). Este relatório visa informar as atividades realizadas conforme determinado pela regulamentação.

2. PERIODO DE REFERÊNCIA

Este relatório tem como período de referência o ano de 2022 e considera os eventos até 31/12/2022.

3. ESTRUTURA - SEGURANÇA DA INFORMAÇÃO DO BANCO MOBILIZE

A segurança da informação segue as diretivas determinadas para o Grupo Renault-Nissan, do qual faz parte o Grupo Mobilize Financial Services e suas subsidiárias entre elas o Banco Mobilize Brasil.

O Banco Mobilize Brasil possui estrutura local onde está alocado o CSI (Correspondente de Segurança da Informação), vinculado funcionalmente à equipe de segurança da Mobilize Financial Services. O CSI é responsável pelo desdobramento das regras de segurança do grupo e pelas adaptações destas regras às necessidades locais, assim como manter a conformidade regulatória e atender as diretrizes de negócio.

Cabe destacar ainda que de acordo com a Política de Segurança da Informação do Grupo todos os usuários dos Sistemas de Informação têm a corresponsabilidade de proteger as informações contribuindo para preservação das atividades do Grupo.

3.1 PARTICIPANTES E SEUS PAPEIS

CISO	Responsável pela definição das políticas e estratégias de segurança da informação do Grupo Mobilize.
Equipe de Segurança da Informação Global	Liderado pelo CISO é responsável pela implantação dos recursos e técnicas de segurança para todas as subsidiárias do Grupo Mobilize.
CSI	Correspondente de Segurança da Informação: responsável pelo desdobramento **das políticas de segurança** da informação da Matriz, implantação das ferramentas de segurança, monitoramento de segurança e treinamentos de segurança de acordo com os padrões definidos pela Matriz. Responde ainda pela análise e proposição de todas as modificações necessárias nos padrões da Matriz para que estejam em conformidade com as exigências locais.

CMSI	É o Corresponsável de Sistemas de Informação (Information Systems Security Métier Co-responsible): Responsável pelo desdobramento das políticas e procedimentos de segurança dentro da sua área de negócio.
Departamento de Proteção e Prevenção (D2P)	Responsável pela definição, manutenção e aplicação da PSSI (Política de Segurança da Informação).
Departamento jurídico	Manutenção das minutas dos contratos que envolvam prestadores de serviços de processamento de dados e armazenamento na nuvem, incluindo clausula para atendimento da Resolução 4658.
Controles internos	Publicar para os públicos interno e externo a Política de Segurança da Informação e Segurança Cibernética em conformidade com a referida resolução.
Tecnologia da informação	Participar das reuniões do grupo de trabalho referente a adequação do banco para atender a referida resolução.
Diretoria de tecnologia da informação	Responsável por suportar, engajar e apoiar a implementação das medidas técnicas e organizacionais para adequação da segurança aos princípios da Política de Segurança Cibernética.

3.2 ÁREA DE SEGURANÇA DA INFORMAÇÃO

Está ligada a Diretoria de Tecnologia da Informação e é coordenada pelo CSI de acordo com as determinações do CISO Mobilize Matriz.

A área de segurança da informação local tem as seguintes atribuições:

Objetivo da missão

- Consistente com as instruções do DSI e os KPIs definidos, contribuir para:
    - Implantar e aplicar a Política de Segurança de Sistemas de Informação de TI / TI do Grupo.
    - Definir e organizar ações de conscientização, treinamento e comunicação sobre segurança de SI / TI.
    - Auxiliar o projeto local de SI / TI no suporte à segurança, garantindo o rascunho dos elementos de segurança associados e alertando o CISO corporativo em caso de não conformidade.
    - Verificar a cobertura dos riscos de segurança de TI / IS com a segurança corporativa de IS / TI com base nas avaliações e nos controles de conformidade.
    - Detectar, alertar a segurança corporativa de IS / TI e coordenar as ações locais em resposta a ataques de TI. Aproveitar as soluções fornecidas em torno desses incidentes.
    - Verificar se a implementação local do DRP está alinhada com a política de DRP do grupo.

- Manter-se informado dos requisitos de segurança resultantes das leis, normas e regulamentos dentro do escopo de sua entidade e garanta a conformidade em colaboração com os negócios e os controles internos.
- Relatar as ações ou necessidades locais relacionadas à segurança de IS / TI ao grupo CISO.

Campos de ação:

- Escopo da organização: subsidiárias
- Escopo geográfico: Brasil
- Escopo técnico: segurança de IS / TI
- Escopo de tempo: ilimitado
- Principais reuniões de decisão: pontos de segurança subsidiários com o grupo CISO.

Entregas e principais indicadores:

- Entregas:
  - Implantação dos textos fundadores (Carta de bom uso, Código de Ética em TI, Política de Segurança,).
  - Avaliação do risco de segurança de SI / TI (de acordo com a avaliação de riscos operacionais de SI).
- Indicadores:
  - Indicadores do país sobre as atividades de segurança de SI / TI e KPI (concebidos com segurança corporativa de SI / TI).

4 AÇÕES REALIZADAS EM 2022

O Banco Mobilize Brasil realizou ações ao longo de 2022, conforme segue:

4.1 MEDIDAS ORGANIZACIONAIS

- Treinamento de Regras de Ouro da Informação para os Colaboradores
- Exercício de Desastre testando a redundância da infraestrutura crítica
- Exercício CyberAttack para treinar a agilidade das equipes
- Revisão do Catálogo de Informação Sensível junto aos departamentos
- Controle das regras de classificação de documentos confidenciais
- Revisão de Acessos de Aplicações Críticas
- Treinamento de Segurança Cibernética para todos os efetivos
- Revisão do Referencial das Aplicações da Mobilize Brasil
- Definição de um Plano de Comunicação de Dicas de Segurança da Informação
- Revalidação da Política de Segurança Cibernética;
- Revalidação do procedimento de respostas a incidentes cibernéticos.
- Revisão e Implantação de Anexo de Segurança para os fornecedores críticos do Banco Mobilize
- Criação e implantação do check-list para revisão anual das respostas aos questionários de segurança para verificar a continuidade da aderência do fornecedor à política de segurança interna.
- Reforço da equipe de Segurança

- Implantação das medidas organizacionais para conformidade com LGPD, especialmente dos conceitos de security by design e security by default;
- Atualização da Plano de Recuperação de Desastres.
- Realização de assessment baseado nas regras NIST para medição da maturidade dos controles de segurança – Holistic – em conjunto com Santander.

4.2 Medidas Técnicas

- Automação da aplicação de patches de segurança em servidores;
- Atualização da ferramenta de antivírus com a implementação do CrowdStrike NGAV;
- Implementação da ferramenta de análise de postura de segurança em cloud TrendMicro;
- Análise para renovação da ferramenta SIEM e equipe SOC com início da implantação da ferramenta Qradar;
- Segregação do ambiente de ferramentas técnicas administrativas dos demais ambientes (dev/prod/hom).
- Atualização do ambiente de Kubernetes;
- Implantação de WAF para aplicações expostas – iniciado e ainda em andamento;
- Simulações de phishing em conjunto com a Matriz utilizando ferramenta Terranova;
- Automação para reciclagem de access Keys no ambiente cloud;
- Substituição da infraestrutura de DR para a aplicação novar 2.0 objetivando ajustar o RPO para o padrão do grupo (15 minutos);
- Aplicação de anonimização em base de dados nos ambientes de homologação;
- Realização de testes de penetração (Pentests) nas principais aplicações web;
- Implementação da ferramenta de classificação de segurança – Bitsight – com rate de 800 pontos.
- Correção de 100% das vulnerabilidades críticas e altas encontrada nas principais aplicações web a partir da realização de pentests e scan de segurança,
- Assessment anti-ransomware;
- Automação do monitoramento dos ambientes críticos;
- Implantação do suporte 24x7 para os ambientes.
- Assessment de Tecnologia: SLA; Gestão de Incidentes; Gestão de Problema; Gestão de Mudança; Gestão de Backup e Restore; Gestão de Risco e Controle; Governança Cloud ; Plano de Continuidade Tecnológica

5 EFETIVIDADE DAS AÇOES REALIZADAS EM 2022

As ações realizadas no ano de 2022 para garantia da segurança cibernética foram efetivas o que se comprova pela não ocorrência de incidentes de segurança nos nossos ambientes.

Das ações realizadas merecem destaque:

- O teste de phishing: este teste, que se repete anualmente, consistiu no envio controlado de e-mails pelo time de segurança da informação para simular phishing e verificar o comportamento dos usuários. O resultado global apresentado pela matriz mostrou que estes testes têm permitido aos usuários maior conscientização quanto à avaliação dos e-mails recebidos pela aplicação dos conhecimentos obtidos nos treinamentos se segurança obrigatórios.
- O teste de Cyber attack: permitiu colocar em prática com os usuários a simulação de um ataque cyber a uma das principais ferramentas da MFS. Neste teste pudemos reforçar os pontos como comunicação e identificar os pontos de melhoria que serão trabalhados em 2023.
- A implementação do Crowdstrike NGAV nos servidores representa também um avanço muito significativo na segurança dos nossos ambientes uma vez que a ferramenta oferece avançados recursos de IA para identificação e bloqueio de eventuais tentativas de intrusão.
- A implantação da ferramenta de medição de segurança Bitsight que apresenta para os interessados o nosso ranking de segurança. Nosso ranking atual é de 800 pontos num máximo de 900, o que representa uma avaliação muito positiva da segurança do nosso ambiente.

Cumprindo exigência da LGPD e GDPR realização ainda na anonimização de dados em ambientes não produtivos e finalizamos os processos de anonimização de dados em ambientes produtivos.

Novamente, a efetividade destas medidas na prevenção de incidentes cibernéticos se observa pela estabilidade do ambiente do Banco Mobilize com relação à segurança cibernética em 2022.

6 INCIDENTES RELEVANTES – PERIODO DE 2022

No período em análise não houve ocorrência de incidentes cibernéticos.

7 RESULTADOS DOS TESTES DE CONTINUIDADE DO NEGÓCIO – BCP

No ano de 2022 o Plano de Continuidade do Negócio foi, mais do que testado, colocado em prática em decorrência da pandemia do COVID-19.

Na prática as ações operacionais e técnicas previstas no BCP se mostraram efetivas e eficazes e puderam impedir qualquer interrupção nas atividades do Banco Mobilize Brasil.

8 GOVERNANÇA DO RELATÓRIO

Este relatório e as evidências de sua validação e apresentação à Direção Geral e as Disposições Gerais - Art. 23 da Resolução n° 4.658 devem estar arquivadas em conjunto e em ambiente seguro pelo período de 5 anos.

TERMO DE AUTENTICIDADE

Eu, Oduvaldo Lara Junior, com inscrição ativa no OAB/SP, sob o n° 232107, inscrito no CPF n° 29169421811, DECLARO, sob as penas da Lei Penal, e sem prejuízo das sanções administrativas e cíveis, que este documento é autêntico e condiz com o original.

IDENTIFICAÇÃO DO(S) ASSINANTE(S)		
CPF	N° do Registro	Nome
29169421811	232107	ODUVALDO LARA JUNIOR

CERTIFICO O REGISTRO EM 20/04/2023 13:16 SOB Nº 20232695270.
PROTOCOLO: 232695270 DE 19/04/2023.
CÓDIGO DE VERIFICAÇÃO: 12305304326. CNPJ DA SEDE: 62307848000115.
NIRE: 41300075336. COM EFEITOS DO REGISTRO EM: 31/03/2023.
BANCO RCI BRASIL S.A.

SEBASTIAO MOTA
SECRETÁRIO-GERAL
www.empresafacil.pr.gov.br