MOBILIZE
FINANCIAL SERVICES

MOBILIZE FINANCIAL SERVICES GROUP

Política de Segurança Cibernética

MFSCYBERP2024- version 2024

MOBILIZE
FINANCIAL SERVICES

Referência	Status	Versão	Idioma	Data da Aplicação	Data da Revisão	Frequência das revisões
MFSCYBERP2024	Approved	2024	PT-BR	05/02/2024	05/02/2025	1 year

Propósito	Em conformidade com o MP1: Suporte e controle RCI, o MP2: Entrega e suporte a sistemas de TI e o MP3: Garantir a segurança dos sistemas, o Grupo de Serviços Financeiros Mobilize define, implementa, verifica e melhora continuamente sua Política de Cibersegurança do Grupo de Serviços Financeiros Mobilize (doravante denominada Política de Cibersegurança). Para garantir a eficácia do sistema de gerenciamento de cibersegurança, o Grupo de Serviços Financeiros Mobilize elabora e atualiza a Política de Cibersegurança. A Política de Cibersegurança estabelece: 1. Os 10 princípios-chave de cibersegurança; 2. Lista de regras bancárias; 3. Regulamentos e leis locais: exemplos de especificidades regulatórias locais; 4. Estrutura para definir objetivos de cibersegurança; 5. Regras de gerenciamento de exceções
Processo de afiliação	MP1: Suporte e controle RCI MP2: Fornecer e dar suporte a sistemas de TI MP3: Garanta a segurança dos sistemas
Destinatários	Grupo de Serviços Financeiros Internos Mobilize
Departamento Emissor	DSI/RRSG
Serviço Emissor	IS Security
Escopo de Aplicação	Todo o grupo Mobilize Financial Services e suas subsidiarias.
Referencias	ISO/IEC 27001 ISO/IEC 27002 ISO/SAE 21434 IEC 62443 NIS2 DORA UNR155 EBA/ACPR Diretrizes

01 PREÂMBULO

O risco cibernético é um grande risco para o Mobilize Financial Services Group. Para controlar-lo o Mobilize Financial Services Group está comprometido em definir, implantar, verificar e melhorar continuamente seu nível de segurança cibernética.

Para alcançar este objetivo primordial, o Mobilize Financial Services Group está empenhado em compreender o seu contexto interno e externo, e em definir e implantar sistemas de gestão de cibersegurança em diferentes áreas de atividade, em função dos riscos, contexto, regulamentos e expectativas das partes interessadas (clientes, investidores, colaboradores, parceiros, autoridades etc.), de acordo com o processo PM01 "Estabelecer os âmbitos dos Sistemas de Gestão da Cibersegurança".

Para garantir a eficácia destes sistemas de gestão da cibersegurança, o Mobilize Financial Services Group define uma estratégia, objetivos e a Política de Cibersegurança do Mobilize Financial Services Group, que constituem a base para todas as suas ações de segurança, de acordo com o processo PM02 "Estabelecer objetivos, estratégia e política de cibersegurança".

Com base nesta estratégia de cibersegurança, nestes objetivos e na política de cibersegurança, o Mobilize Financial Services Group está continuamente trabalhando para definir, implementar, verificar e melhorar todos os processos que lhe permitam controlar todos os riscos de cibersegurança para cada um dos sistemas de gestão de cibersegurança em vigor, de acordo com o processo PM03 Gerir um sistema de gestão de cibersegurança.

De acordo com o processo PM02 "Estabelecer objetivos, estratégia e política de cibersegurança", o Mobilize Financial Services Group define, implanta, verifica e melhora continuamente a Política de Cibersegurança do Mobilize Financial Services Group (doravante a Política de Segurança Cibernética).

A Política de Cibersegurança estabelece:

1. Os 10 princípios-chave da cibersegurança;
2. Lista de regras bancárias;
3. Regulamentos e leis locais: exemplos de especificidades regulatórias locais;
4. Quadro para a definição de objetivos de cibersegurança;
5. Regras de gerenciamento de exceções

02 DECLARAÇÃO DE SEGURANÇA CIBERNÉTICA DO GRUPO MOBILIZE FINANCIAL SERVICES

[PALAVRAS DO CEO]

03 APRESENTAÇÃO DA POLÍTICA CIBERNÉTICA

1. PROPOSITO

Ataques cibernéticos e falhas de sistemas de informação são um grande risco para o Mobilize Financial Services Group, bem como riscos ligados ao aquecimento global, falhas na cadeia de suprimentos, instabilidade geopolítica e condições econômicas.

Esse risco, se quando materializado, pode ter um efeito adverso na segurança e privacidade dos clientes, no desempenho, nos ativos, nas operações de negócios, na imagem ou no alcance de seus objetivos do Mobilize Financial Services Group.

De forma a controlar o risco de ciberataque e falha dos sistemas de informação, o Mobilize Financial Services Group estabelece, implementa, mantém e melhora continuamente os Sistemas de Gestão de Cibersegurança (SGC) adaptados à sua estrutura, atividades e Produtos com Elementos Digitais, e aos riscos que pesam sobre as suas atividades e Produtos com Elementos Digitais.

Para este fim, o Mobilize Financial Services Group está comprometido em controlar os riscos que afetam a disponibilidade, integridade e confidencialidade de seus dados, processos de negócios e Produtos com Elementos Digitais, de acordo com os danos potenciais para o Mobilize Financial Services Group, suas subsidiárias e afiliadas e, quando aplicável, para outros (clientes, usuários da externos, etc.).

Para garantir a eficácia do sistema de gestão da cibersegurança, o Mobilize Financial Services Group elabora e atualiza a Política de Cibersegurança.

A atual Política de Cibersegurança foi elaborada com base nos princípios e melhores práticas descritos na estrutura global de Política de Cibersegurança criada pelo Grupo Renault. Essa abordagem garante que o Mobilize Financial Services Group não esteja apenas alinhado com a estrutura de segurança cibernética do Grupo Renault, mas também reflita os requisitos específicos aplicáveis ao escopo bancário e às regulamentações e leis locais em cada país.

A Política de Cibersegurança estabelece as bases para a gestão da cibersegurança do Mobilize Financial Services Group, estabelecendo 10 princípios:

- Princípio 1: Garantir uma governança eficiente da cibersegurança;
- Princípio 2: Garantir o envolvimento de todos na cibersegurança;
- Princípio 3: Garantir a segurança cibernética controlada com base nos riscos;
- Princípio 4: Garantir a integração da cibersegurança em todos os Produtos com Elementos Digitais (segurança por design e por padrão);
- Princípio 5: Garantir o conhecimento e o controle dos ativos;
- Princípio 6: Garantir o acesso seguro aos ativos;
- Princípio 7: Garantir a securitização de ativos;
- Princípio 8: Garantir o cumprimento e a melhoria contínua da cibersegurança;
- Princípio 9: Garantir a gestão de incidentes cibernéticos;
- Princípio 10: Garantir a continuidade dos negócios e a gestão de crises.

A Política de Cibersegurança contribui para o respeito dos regulamentos internacionais e nacionais a que uma ou mais entidades do Grupo estão sujeitas, em particular regulamentos relacionados com:

- a cibersegurança das atividades do Mobilize Financial Services Group;
- regulamentos relacionados à cibersegurança de seus Produtos com Elementos Digitais e serviços;
- regulamentos relacionados à proteção de dados pessoais;
- regulamentos relacionados com a proteção da propriedade intelectual e dos direitos de autor.

Os princípios não são independentes, mas conectados entre si e devem ser interpretados em conjunto, de modo que:

- O princípio 1 trata da governança geral da segurança cibernética. Este princípio impõe e controla os outros princípios;
- O Princípio 2 estabelece os fundamentos relativos à gestão de Recursos Humanos necessários para contribuir eficazmente para a cibersegurança e a gestão de riscos cibernéticos do Grupo Mobilize Financial Services;
- O princípio 3 estabelece as regras para a gestão de toda a cibersegurança em relação aos riscos cibernéticos;
- O princípio 4 é um princípio fundamental, na medida em que exige que os proprietários de produtos e os gestores de produtos respeitem todos os outros princípios e, em particular, o princípio 3, que estabelece as regras para a gestão de riscos cibernéticos.

2. ESCOPO APLICÁVEL

A Política de Cibersegurança aplica-se a todos os sistemas de informação implementados para as atividades do Mobilize Financial Services Group, seja pelo Mobilize Financial Services Group ou suas subsidiárias integradas, e sistemas de informação do Mobilize Financial Services Group Products with Digital Elements.

Qualquer pessoa dentro do Grupo Mobilize Serviços Financeiros envolvida na concepção, produção, administração, manutenção, controle e/ou desmantelamento da totalidade ou parte dos sistemas de informação implementados para as atividades do Grupo Mobilize Serviços Financeiros ou, sistemas de informação de Produtos com Elementos Digitais tem o dever reforçado de respeitar e garantir o respeito da Política de Cibersegurança do Grupo Mobile Serviços Financeiros, as regras organizacionais e técnicas de Cibersegurança e os processos que dela derivam.

Todos os indivíduos, internos ou externos ao Mobilize Financial Services Group, que sejam partes interessadas dos sistemas de informação exigidos pelas atividades do Mobilize Financial Services Group, devem respeitar os princípios de Cibersegurança da Política de Cibersegurança do Mobilize Financial Services Group, as regras organizacionais e técnicas de cibersegurança e os processos que dela derivam.

Os proprietários da totalidade ou de parte de um sistema de informação (Product Owners) garantem contratualmente, com o apoio do(s) Departamento(s) do Grupo de Serviços Financeiros em causa responsável pelas Compras, Departamento(s) responsável(is) pelo Jurídico e pelo(s) Departamento(s) responsável(is) pela Cibersegurança, que os fornecedores e fornecedores, cujos Produtos com Elementos Digitais e/ou serviços possam prejudicar as atividades e Produtos do Grupo de Serviços Financeiros com Elementos Digitais, estão de acordo com os requisitos da Política de Cibersegurança do Grupo Mobilize Financial Services, as regras organizacionais e técnicas de Cibersegurança e os processos que dela derivam.

3. APLICABILIDADE

Para garantir a conformidade com os 10 princípios-chave da Política de Cibersegurança (cf. capítulo 04), estes são especificados pelas regras organizacionais e técnicas de Cibersegurança definidas e revisadas considerando as mudanças na estratégia do Mobilize Financial Services Group, regulamentos, estado da arte, vulnerabilidades, ameaças e riscos cibernéticos.

O Mobilize Financial Services Group assegura a definição, implantação e melhoria contínua de todos os processos de gestão, operacionais e de suporte, conforme necessário, para garantir o cumprimento das regras organizacionais e técnicas e a eficiência operacional.

O cumprimento dos requisitos da Política de Cibersegurança do Grupo Mobilize Financial Services, das regras organizacionais e técnicas de Cibersegurança e dos processos que dela derivam deve ser continuamente monitorizado para garantir que os níveis de Cibersegurança estão alinhados com os objetivos e a estratégia.

O Mobilize Financial Services Group garante que os processos sejam documentados e estejam sempre acessíveis quando estes documentos:

- são exigidos pela regulamentação aplicável,
- requeridos pelos organismos de certificação,
- contribuem de várias formas para os objetivos do Grupo de Serviços Financeiros,
- contribuem para a melhoria da eficiência dos processos.

4. REGRAS ORGANIZACIONAIS E TÉCNICAS DE CIBERSEGURANÇA

Para a implementação efetiva da Política de Cibersegurança, o Mobilize Financial Services Group define e implanta regras organizacionais e técnicas de segurança cibernética adaptadas ao contexto regulatório e de negócios.

As regras organizacionais e técnicas são adaptadas ao contexto da seguinte forma:

- Regras organizacionais e técnicas comuns devem ser especificadas e aplicáveis a todo o Grupo pelo Diretor de Segurança da Informação do Grupo Mobilize Financial Services;
- Se uma regra não for adequada para um determinado setor de negócio, o Líder de Gestão de Cibersegurança de Domínio responsável pela cibersegurança desse setor de negócio, com o apoio do Diretor de Segurança da Informação do Grupo Mobilize Financial Services, deve implementar e implementar uma regra específica que seja mais adequada à situação;
- Se uma lei local impuser medidas de cibersegurança mais rigorosas, o Correspondente de Segurança Local, com o apoio do Diretor de Segurança da Informação do Grupo Mobilize Financial Services e do Líder de Gestão de Cibersegurança de Domínio responsável pela cibersegurança para este setor de negócios, implementará uma regra local mais apropriada.

Assim, o Mobilize Financial Services Group define regras organizacionais e técnicas adaptadas para garantir a resiliência das atividades e produtos do Mobilize Financial Services Group com elementos digitais contra riscos cibernéticos, aplicáveis a:

- sistemas de informação compartilhados exigidos pelas operações e atividades do Mobilize Financial Services Group,
- sistemas de informação específicos das entidades bancárias,
- sistemas de informação específicos para os serviços de cibersegurança.

5. APPROVAÇÃO

Ao nível do Grupo Mobilize Serviços Financeiros, a Política de Cibersegurança do Grupo Mobilize Serviços Financeiros deve ser validada pelo Chief Information Officer e Chief Risk Officer do Mobilize Financial Services Group e aprovada pelo Conselho de Supervisão do Grupo Mobilize Financial Services (membros do Comité de Risco) e pelo Conselho Executivo (ComEx).

6. REVISÃO

A Política de Cibersegurança do Grupo Mobilize Financial Services deve ser revista pelo menos todos os anos ou em cada evolução significativa em contextos internos e/ou externos, necessidades das partes interessadas, estratégia corporativa ou riscos cibernéticos, conforme necessário.

04 AS 10 PRINCIPAIS CHAVES DA SEGURANÇA CIBERNÉTICA DA MOBILIZE FINANCIAL SERVICES GROUP

Principle 1 Assegurando a eficiência da governança da segurança cibernética

1.1 GOV-LDSHP Regras para a Liderança da Equipe de Suporte

1.1.1 GOV-LDSHP-1 Uma governança de segurança cibernética eficaz é um pré-requisito para a proteção contra riscos, categorizados como principais riscos no Mobilize Financial Services Group.

1.1.2 GOV-LDSHP-2 Para tanto, a Equipe de Liderança deverá:

- Nomear um Diretor de Segurança da Informação para o Mobilize Financial Services Group (doravante CISO)
- Ser treinado e garantir que o pessoal do Grupo de Serviços Financeiros da Mobilize, dependendo das missões confiadas, seja adequadamente treinado para adquirir o conhecimento e as habilidades necessárias para entender as questões de segurança cibernética, moldar e avaliar os riscos e seus impactos nos produtos do Grupo de Serviços Financeiros da Mobilize com Elementos, serviços e/ou atividades digitais,
- Aprovar, comunicar amplamente e disponibilizar a Política e as regras de Segurança Cibernética e garantir que todas as pessoas que projetam, implementam, mantêm e/ou usam sistemas de informação estão cientes das apostas, têm uma compreensão clara de seu conteúdo e o aplicam,
- Aprovar o Roteiro Anual de Cibersegurança que implementa os objetivos e a estratégia de cibersegurança do Mobilize Financial Services Group e prestar apoio comunicando esses objetivos e estratégia e alocando os recursos (incluindo humanos, financeiros e de apoio) necessários para alcançar os objetivos estabelecidos em um tempo viável;
- Garantir que os processos de gestão da cibersegurança sejam estabelecidos e atualizados para gerir eficazmente os riscos,
- Garantir que as funções e responsabilidades dos envolvidos na cibersegurança do Mobilize Financial Services Group estão claramente definidas, ainda relevantes e atualizadas,
- Garantir que os comitês necessários para a gestão da segurança cibernética estejam definidos e operacionais,
- Garantir que todos os processos operacionais cumprem continuamente a Política de Cibersegurança e as regras organizacionais e técnicas de cibersegurança,
- Garantir que o modelo de governança de segurança cibernética do Mobilize Financial Services Group seja implementado em nível de grupo, entidade e local (abordagem One Cybersecurity approach).

1.2 GOV-ORGAN Regras organizacionais , funções e responsabilidades da segurança cibernética

1.2.1 GOV-ORGAN-1 O CISO deve definir, implantar, verificar a eficácia e melhorar os processos de gestão da cibersegurança.

1.2.2 GOV-ORGAN-2 O CISO, com o apoio do(s) Departamento(s) responsável(is) pelos Recursos Humanos, deve criar equipes com competências relevantes para o apoiar nas suas missões e uma rede para implementar a política e os processos de cibersegurança em todas as unidades de negócio e subsidiárias integradas do Mobilize Financial Services Group.

1.2.3 GOV-ORGAN-3 O CISO deve definir funções e responsabilidades para as principais missões de cibersegurança, garantindo que as áreas ou tarefas potencialmente conflitosas sejam mantidas separadas. Se a segregação não for possível, o CISO deve assegurar que o papel seja monitorado.

1.2.4 GOV-ORGAN-4 O CISO deve criar comitês estratégicos e operacionais para gerenciar as questões de segurança cibernética do Mobilize Financial Services Group.

1.2.5 GOV-ORGAN-5 Sob a supervisão da Equipe de Liderança, o CISO deverá:

- Ter a abrangência dos diversos sistemas de gestão de cibersegurança para garantir a cibersegurança de todas as atividades e Produtos com Elementos Digitais;
- Para cada um, nomeie um piloto encarregado de montá-lo, executá-lo, verificar seu funcionamento, melhorá-lo.

1.2.6 GOV-ORGAN-6 O CISO deve assegurar que os Princípios da Política de Cibersegurança são implementados através de processos de cibersegurança conformes e eficazes, em particular:

- Processo(s) de governança;
- Processo(s) de gestão de riscos;
- Processo(s) de gestão de recursos humanos, incluindo formação e sensibilização em cibersegurança;
- Processo(s) de gestão de ativos;
- Processo(s) de gerenciamento de acesso seguro;
- Processo(s) de segurança física e ambiental;
- Processo(s) de segurança operacional;
- Processo(s) de segurança de rede;
- Processo(s) para segurança de aquisição, desenvolvimento e manutenção, incluindo tratamento e divulgação de vulnerabilidades;
- Processo(s) de utilização de criptografia;
- Processo(s) de segurança da cadeia de suprimentos;
- Processo(s) de gerenciamento de incidentes;
- Processo(s) de continuidade de negócios;
- Processo(s) de gestão de crises.

1.2.7 GOV-ORGAN-7 Todo processo de cibersegurança deve ter um Proprietário do Processo designado.

1.2.8 GOV-ORGAN-8 Na ausência de um Proprietário de Processo designado, o CISO deve garantir que um novo Proprietário de Processo, no nível certo, seja nomeado o mais rápido possível.

1.2.9 GOV-ORGAN-9 O Proprietário do Processo deve definir, implantar, verificar a conformidade e a eficiência e melhorar continuamente o processo pelo qual é responsável.

1.2.10 GOV-ORGAN-10 O CISO verifica a coerência global da governança da cibersegurança, bem como a conformidade e a eficácia dos sistemas de gestão da cibersegurança.

1.2.11 GOV-ORGAN-11 O CISO deve assegurar que os sistemas de gestão da cibersegurança são continuamente melhorados e que as não conformidades identificadas durante as auditorias são abordadas e tratadas.

1.2.12 GOV-ORGAN-12 O CISO deve assegurar todos os esforços para lidar com incidentes de cibersegurança.

1.2.13 GOV-ORGAN-13 O CISO informará a Equipe de Liderança sobre o estado geral dos sistemas de informação, o seu nível de conformidade e eficiência, a medida em que os objetivos que lhe foram definidos são alcançados e o estado dos riscos que pesam sobre o Grupo Mobilize Serviços Financeiros e proporá ações a implementar para melhorar o nível de cibersegurança do Grupo Mobilize Serviços Financeiros.

1.2.14 GOV-ORGAN-14 O CISO deve definir, implantar, verificar e melhorar continuamente um programa de comunicação sobre segurança cibernética do Mobilize Financial Services Group, para funcionários internos, fornecedores, clientes, CSIRTs ou autoridades, levando em consideração a sensibilidade da informação a ser transmitida, requisitos operacionais e obrigações regulatórias.

Principle 2 Garantir o Envolvimento de todos na Segurança Cibernética

2.1 HR-SKILL Regras de Sensibilização e Competencias

2.1.1 HR-SKILL-1 O(s) departamento(s) responsável(is) pelos Recursos Humanos deve assegurar que as pessoas às quais são atribuídas funções e responsabilidades de cibersegurança tenham as competências, a consciência, a ética e a probidade para as cumprir.

2.1.2 HR-SKILL-2 Para garantir a competência dos colaboradores, o(s) Departamento(s) responsável(is) pelos Recursos Humanos define, implementa, verifica e melhora continuamente um programa de gestão de competências para garantir que os colaboradores envolvidos na cibersegurança, independentemente do seu nível de envolvimento, tenham continuamente as competências, consciência, ética e probidade necessárias para cumprir a sua missão.

2.1.3 HR-SKILL-3 Além disso, o(s) departamento(s) responsável(is) pelos Recursos Humanos devem assegurar que os funcionários que iniciam um turno de carreira sejam submetidos aos treinamentos de segurança cibernética necessários para garantir que estejam totalmente operacionais em suas novas funções e responsabilidades.

2.1.4 HR-SKILL-4 O(s) departamento(s) responsável(is) pelos Recursos Humanos deve fornecer formação específica aos gestores da Equipe de Liderança e do Grupo de Serviços Financeiros da Mobilize para lhes permitir adquirir conhecimentos e competências para poderem compreender as questões de cibersegurança, moldar e avaliar os riscos e os seus impactos nos produtos, serviços e/ou atividades do Grupo de Serviços Financeiros Mobilize com Elementos Digitais, serviços e/ou atividades.

2.1.5 HR-SKILL-5 O(s) Departamento(s) responsável(is) pelos Recursos Humanos deve assegurar que todos os funcionários do Mobilize Financial Services Group, independentemente do seu trabalho, sejam informados dos desafios da cibersegurança, das ameaças que o Mobilize Financial Services Group enfrenta, dos riscos associados a essas ameaças, do impacto potencial em caso de incidentes e das melhores práticas para prevenir a ocorrência de tais incidentes.

2.1.6 HR-SKILL-6 O(s) Departamento(s) responsável(is) de Recursos Humanos acompanhará e documentará os programas de sensibilização e treinamento e sua efetividade, observadas as normas da legislação trabalhista vigente.

2.1.7 HR-SKILL-7 Os prestadores de serviços devem aumentar a conscientização e treinar seus funcionários ao trabalhar nos sistemas de informação do Mobilize Financial Services Group ou ao analisar um nível de segurança cibernética do Mobilize Financial Services Group. A sensibilização e a formação devem ser adaptadas à missão do trabalhador.

2.1.8 HR-SKILL-8 O(s) Departamento(s) responsável(is) de Recursos Humanos, com o apoio do(s) Departamento(s) responsável(is) pela área Jurídica e pelo(s) Departamento(s) responsável(is) pela Cibersegurança, elaborará, publicará e comunicará a Carta do Grupo Renault para a utilização dos recursos de SI e ferramentas digitais, em conformidade com a legislação laboral. Esta carta estabelecerá os usos autorizados e proibidos de recursos de Tecnologia da Informação e ferramentas digitais e as penalidades em caso de descumprimento desses requisitos.

2.2 HR-OBLIG Obrigações das pessoas que colocam em causa a segurança cibernética da Mobilize Financial Services Group

2.2.1 HR-OBLIG-1 Cada funcionário do Mobilize Financial Services Group deve cumprir os Princípios da Política de Segurança Cibernética, as regras organizacionais e técnicas de segurança cibernética, independentemente de sua função e responsabilidades. Da mesma forma, ele deve aplicar a Carta do Grupo Renault para o uso de recursos de SI e ferramentas digitais durante toda a duração de seu contrato de trabalho.

NOTA: Os funcionários do Grupo de Serviços Financeiros Mobilize que violarem qualquer uma dessas regras são responsáveis pelos danos resultantes e podem ser sancionados proporcionalmente de acordo com a Carta.

2.2.2 HR-OBLIG-2 Todo funcionário da Mobilize Financial Services deve impor o sigilo de segurança cibernética mesmo após o término de seu contrato de trabalho. O conhecimento adquirido através do exercício das funções e responsabilidades atribuídas não deve ser usado contra os interesses do Mobilize Financial Services Group nem ameaçar as operações e atividades do Mobilize Financial Services Group de qualquer forma.

2.2.3 HR-OBLIG-3 Os prestadores de serviços devem comunicar os Princípios da Política de Cibersegurança do Grupo Mobilize Financial Services, as regras organizacionais e técnicas de cibersegurança relevantes para a missão confiada e a Carta do Grupo Renault para a utilização de recursos e ferramentas digitais do SI aos seus colaboradores que intervenham de alguma forma nos sistemas de informação do Grupo Mobilize Financial Services ou na conceção, fabricação, venda ou pós-venda de um Produto com Elementos Digitais (por exemplo, carros, produtos para mobilidade, estação de carregamento...).

NOTA: Se os funcionários de um prestador de serviços violarem estas regras, este prestador de serviços pode estar sujeito às sanções previstas contratualmente.

Principle 3 Garantir a segurança cibernética controlada com base em riscos

3.1 RSK-MANAG Regras para a gestão de riscos

3.1.1 RSK-MANAG-1 Para mitigar os riscos de cibersegurança e otimizar os controles de cibersegurança, o CISO, com o apoio do(s) Departamento(s) responsável(is) pela Cibersegurança, define, implanta, verifica a eficácia e melhora continuamente um processo de gestão de riscos que inclui as seguintes atividades:

- Identificar riscos
- Analisar os riscos
- Avaliar riscos
- Tratar riscos

Para a avaliação de risco do produto, o processo pode fornecer diferentes níveis de avaliação, dependendo da criticidade dos Produtos com Elementos Digitais e da sensibilidade dos dados processados (por exemplo, configurador de segurança, avaliação de risco de alto nível, avaliação de risco simplificada, avaliação de risco detalhada).

3.1.2 RSK-MANAG-2 Esse processo é projetado para gerenciar todos os riscos de segurança, privacidade de dados, financeiros, operacionais e de imagem que afetam as atividades, produtos com elementos digitais, serviços e dados do Mobilize Financial Services Group (comumente chamados de ativos primários).

3.1.3 RSK-MANAG-3 Para uma gestão eficaz dos riscos, o(s) departamento(s) responsável(is) pela cibersegurança deve definir as funções e responsabilidades das partes interessadas, em particular os proprietários de riscos, os proprietários de produtos, os gestores de produtos e os responsáveis pela realização de avaliações de riscos e pela monitorização do tratamento dos riscos.

3.1.4 RSK-MANAG-4 Além disso, devem ser criados comités de gestão de riscos, nomeadamente para a gestão de riscos elevados e a avaliação do cumprimento e da eficácia do processo de gestão de riscos.

3.1.5 RSK-MANAG-5 Para garantir a sua eficácia, seja qual for a atividade a avaliar, o(s) Departamento(s) responsável(is) pela Cibersegurança deve definir e implementar critérios de avaliação de risco, impacto e aceitação que possam ser adaptados ao ambiente operacional analisado (por exemplo, tecnologia da informação, aplicações de tecnologia bancária ou operacional ou objetos conectados).

3.1.6 RSK-MANAG-6 O(s) departamento(s) responsável(is) pela Segurança Cibernética definirá e implantará catálogos para capitalizar o conhecimento e otimizar a identificação, análise e avaliação de riscos, e que serão alimentados com as conclusões das avaliações de risco e outras fontes relevantes.

3.1.7 RSK-MANAG-7 O(s) departamento(s) responsável(is) pela Cibersegurança deve definir regras e modelos para documentar as avaliações de risco.

3.1.8 RSK-MANAG-8 O(s) departamento(s) responsável(is) pela Cibersegurança deve assegurar que as informações sobre vulnerabilidades, ameaças, riscos e planos de reparação sejam comunicadas apenas às pessoas que tenham necessidade de saber.

3.1.9 RSK-MANAG-9 As avaliações de risco devem ser atualizadas periodicamente e sempre que sejam identificadas alterações no âmbito, tecnologias, vulnerabilidades ou ameaças, a fim de garantir que os riscos sejam mantidos sob controle ao longo do tempo.

Principle 4 Garantir a integração da segurança cibernética em todos os produtos com elementos digitais (segurança por design e por padrão)

Para este Princípio, os requisitos referem-se a outros princípios e estabelecem os papéis e responsabilidades das partes interessadas no projeto para garantir que todos os princípios sejam respeitados desde a fase de projeto até o descomissionamento. Este Princípio garante a Cibersegurança por conceção e a Cibersegurança ao longo do tempo.

4.1 INT-RESPO Regras e Responsabilidades

4.1.1 INT-RESPO-1 O Product Owner é responsável, em nome do Risk Owner, com o apoio do Product Manager, por implementar todas as medidas necessárias para manter os riscos sob controle relativos ao Produto com Elementos Digitais, às necessidades internas ou colocados no mercado, pelos quais ele / ela é responsável, e garantir a segurança por design e por padrão.

4.1.2 INT-RESPO-2 O(s) departamento(s) responsável(is) pelo Desenvolvimento de Produto com Elementos Digitais, quer desenvolvidos para uso interno quer para serem colocados no mercado, devem assegurar que as regras deste Princípio sejam integradas nos seus processos de gestão de projetos para assegurar os Produtos com Elementos Digitais desenvolvidos pelas suas Equipes.

4.2 INT-MGRSK Regras para a identificação de ativos e gestão de riscos com medidas de cibersegurança

4.2.1 INT-MGRSK-1 O Product Owner deve identificar o valor dos Ativos Primários (processos e dados processados) para determinar os requisitos de disponibilidade, integridade, confidencialidade, autenticidade, rastreabilidade e não repúdio, com a ajuda do Gerente de Produto.

4.2.2 INT-MGRSK-2 O Product Owner deve garantir que o Product Manager defina, documente e mantenha atualizada toda a arquitetura do produto e atualize todas as bases de conhecimento de ativos (por exemplo, Bancos de Dados de Gerenciamento de Configuração).

4.2.3 INT-MGRSK-3 Desde o início do projeto, o Gerente de Produto, em nome do Product Owner, deve realizar uma avaliação baseada em riscos para identificar, analisar e avaliar riscos e definir um plano de segurança cibernética para controlar os riscos que possam afetar a disponibilidade, integridade, confidencialidade, autenticidade, rastreabilidade e/ou não repúdio de processos e dados processados.

4.2.4 INT-MGRSK-4 O Gestor de Produto deve atualizar periodicamente a avaliação baseada nos riscos para garantir que os riscos estão sob controle ao longo do ciclo de vida dos Produtos com Elementos Digitais.

4.2.5 INT-MGRSK-5 O Gerente de Produto deve atualizar a avaliação baseada em risco quando o Produto com Elementos Digitais estiver sujeito a alterações importantes (por exemplo, alteração de arquitetura).

4.2.6 INT-MGRSK-6 Quando for identificado um novo risco, ou se o risco aumentar na sequência de uma avaliação atualizada baseada no risco, o gestor de produto deve definir e aplicar um novo plano de redução dos riscos.

4.3 INT-DEVLP Regras para desenvolvimento

4.3.1 INT-DEVLP-1 O Gestor de Produto deve assegurar que os Produtos com desenvolvimento da Digital Elements, sejam eles próprios ou subcontratados, cumprem as regras do Mobilize Financial Services Group em termos de desenvolvimento para garantir o nível de cibersegurança do sistema de informação.

4.3.2 INT-DEVLP-2 O Gerente de Produto deve garantir que os desenvolvimentos sejam seguros, realizando revisões de código e revisões de arquitetura durante toda a fase de desenvolvimento.

4.3.3 INT-DEVLP-3 O Gestor de Produto deve assegurar que apenas os dados de teste sem dados pessoais e dados sensíveis sejam processados para desenvolvimento e teste, exceto no caso de derrogações devidamente autorizadas pelo(s) Departamento(s) responsável(is) pela Cibersegurança.

4.4 INT-ACQUI Regras para a aquisição de produtos com elementos ou componentes digitais ou o uso de um fornecedor de serviços.

4.4.1 INT-ACQUI-1 Ao utilizar serviços, componentes e/ou Produtos externos com Elementos Digitais, o Product Owner deve garantir que os fornecedores e/ou vendedores ofereçam, em todos os momentos, um nível de proteção em termos de disponibilidade, integridade, confidencialidade, autenticidade, rastreabilidade e não repúdio pelo menos equivalente aos identificados ao identificar o valor dos Ativos Primários.

4.4.2 INT-ACQUI-2 O Product Owner deve garantir que os contratos com fornecedores e vendedores autorizem o Grupo Mobilize Financial Services a verificar, a qualquer momento, se cumprem os requisitos contratualmente acordados de cibersegurança.

4.5 INT-COMMT Regras para definir o papel dos comitês de gerenciamento de projetos

4.5.1 INT-COMMT-1 Os comités de gestão de projetos devem assegurar que esta avaliação baseada no risco é realizada de forma adequada e que as ações estabelecidas no plano de cibersegurança são devidamente executadas.

4.5.2 INT-COMMT-2 Se identificar a não execução da avaliação baseada no risco ou o não cumprimento do plano de cibersegurança, os Comitês de Gerenciamento de Projeto devem lembrar imediatamente o Product Owner e o Product Manager de suas obrigações, informar o Risk Owner e impedir que o projeto entre em produção até que tenha sido colocado em conformidade.

4.6 INT-OPERT Regras para Operação

4.6.1 INT-OPERT-1 O Gerente de Produto deve definir, documentar e atualizar todas as regras e procedimentos operacionais relacionados ao seu Produto com Elementos Digitais, seja no local ou na Nuvem, e, em particular, especificar os seguintes elementos:

- Instalação e configuração do Sistema Manual
- Gestão de acesso e rastreabilidade
- Backups
- Gerenciamento de capacidade
- Gestão de incidentes
- Gerenciamento técnico de vulnerabilidades
- Procedimentos de reinicialização e recuperação do sistema

- Supervisão
- Gestão da obsolescência
- Disposição

4.6.2 INT-OPERT-2 O Gerente de Produto deve adaptar o dimensionamento do sistema e antecipar desenvolvimentos futuros para garantir o desempenho, a manutenção e a disponibilidade do sistema ao longo do tempo.

4.6.3 INT-OPERT-3 O Gerente de Produto deve criar ambientes separados para desenvolvimento, teste e operação, e garantir a segurança cibernética de todos esses ambientes para reduzir os riscos de acesso e modificação não autorizados.

4.6.4 INT-OPERT-4 O Gerente de Produto deve revisar periodicamente e atualizar os direitos de acesso ao Produto com Elementos Digitais para garantir que apenas as pessoas certas tenham acesso.

4.6.5 INT-OPERT-5 O Gerente de Produto deve garantir que o código-fonte seja protegido e acessível apenas a pessoas autorizadas e que esse acesso seja registrado.

4.6.6 INT-OPERT-6 O Gerente de Produto deve garantir que as soluções de proteção contra malware e negação de serviço sejam implantadas no Produto com ativos do Digital Elements.

4.6.7 INT-OPERT-7 O Gerente de Produto deve garantir que os backups sejam feitos regularmente e com segurança, para que os sistemas possam ser recuperados em caso de incidente.

4.6.8 INT-OPERT-8 Em caso de obsolescência, o gestor de produto deve pôr em prática um plano de gestão da obsolescência para substituir a componente obsoleta ou implementar medidas de cibersegurança reforçadas para o elemento obsoleto, a fim de reduzir o risco associado ao mesmo.

4.7 INT-VLNMG Regras para gerenciamento de vulnerabilidade e conformidade em todo o ciclo de vida do produto com elementos digitais

4.7.1 INT-VLNMG-1 Ao longo do ciclo de vida dos Produtos com Elementos Digitais, desde a concepção até ao descomissionamento, o Gestor de Produto, com o apoio do(s) Departamento(s) responsável(is) pela Cibersegurança e, se necessário, do(s) Departamento(s) responsável(is) pela Segurança Física e/ou Departamento(s) responsável(is) pela Engenharia, verificará periodicamente a cibersegurança técnica dos Produtos com Elementos Digitais através de avaliações técnicas de cibersegurança e/ou testes de penetração, em conformidade com as regras técnicas de auditoria.

4.7.2 INT-VLNMG-2 O Gerente de Produto deve implementar uma política de manutenção do Produto com Elementos Digitais para garantir que o Produto com Elementos Digitais seja atualizado e compatível o mais rápido possível, durante todo o seu ciclo de vida.

4.7.3 INT-VLNMG-3 Quando uma nova vulnerabilidade é identificada no Produto com Elementos Digitais, o Gerente de Produto deve atualizar a avaliação baseada no risco e, se necessário, implementar um plano de segurança cibernética atualizado para lidar com esses riscos.

4.8 INT-CONTI Regras para a continuidade, incidente, e gestão de crise

4.8.1 INT-CONTI-1 O Gerente de Produto deve estabelecer um Plano de Recuperação de Desastres para superar incidentes. Esse plano é elaborado de acordo com o valor dos processos e dados tratados, e a necessidade de disponibilidade e integridade.

4.8.2 INT-CONTI-2 Para garantir a continuidade dos negócios, o Gerente de Produto deve garantir que os sistemas de comutação e recuperação estejam em vigor e operacionais para garantir a eficácia do Plano de Recuperação de Desastres.

4.8.3 INT-CONTI-3 O Gerente de Produto deve testar periodicamente o funcionamento correto dos sistemas de comutação e recuperação e o Plano de Recuperação de Desastres.

4.8.4 INT-CONTI-4 Em caso de não operação, o Gerente de Produto deve fazer quaisquer melhorias relevantes nos sistemas de comutação e recuperação e no Plano de Recuperação de Desastres, e testá-los novamente para validar sua operação.

4.8.5 INT-CONTI-5 O Gestor de Produto deve transmitir informações, em particular documentos técnicos de arquitetura, avaliação baseada no risco e registos de cibersegurança, e configurar interações relevantes para permitir que o(s) departamento(s) responsável(is) pela cibersegurança detete eventos temidos, analise e avalie os seus impactos para responder a incidentes de cibersegurança.

4.8.6 INT-CONTI-6 Em caso de incidente, o Product Owner, com o apoio do Gerente de Produto e do(s) Departamento(s) responsável(is) pela Cibersegurança e, se necessário, do(s) Departamento(s) responsável(is) pela Segurança Física e/ou Departamento(s) responsável(is) pela Engenharia, deverá fazer o possível para conter o incidente, encontrar e entender as causas do incidente, corrigir as vulnerabilidades envolvidas e, se necessário, fortalecer a segurança cibernética de seu produto com elementos digitais.

Principle 5 Garantir o conhecimento e controle dos ativos

5.1 AST-MANAG Regras para a gestão de ativos

5.1.1 AST-MANAG-1 O(s) departamento(s) responsável(is) pelo Inventário de Ativos deve configurar e gerenciar os Bancos de Dados de Gerenciamento de Configuração para garantir o conhecimento dos Ativos Primários internos e terceirizados (processos e dados de negócios) e dos Ativos de Suporte internos e externos (em particular instalações, hardwares, softwares, redes) e suas interações, incluindo informações sobre os proprietários de ativos e regras de utilização de ativos, quer se trate dos sistemas de informação do Grupo de Serviços Financeiros Mobilize ou de seus Produtos com Elementos digitais no mercado.

5.1.2 AST-MANAG-2 Os Bancos de Dados de Gerenciamento de Configuração devem garantir um alto nível de confidencialidade, de modo que apenas o pessoal autorizado tenha acesso às informações confidenciais que contém.

5.1.3 AST-MANAG-3 Para Produtos com Elementos Digitais envolvidos na totalidade ou em parte de um processo de negócio, as Bases de Dados de Gestão de Configuração devem conter, para além das informações habituais, pelo menos, as seguintes informações atualizadas sobre cibersegurança de ativos:

- A identidade do Product Owner e do seu departamento;
- A identidade do Gerente de Produto e seu departamento;
- A identidade do Proprietário do Risco;
- Criticidade do ativo;

- A lista de dados tratados pelo ativo com informações sobre necessidade de confidencialidade e características (por exemplo, dados pessoais);
- Informações sobre ciclo de vida;
- Processos de negócio em que o ativo está envolvido;
- Datas e validade da última avaliação de risco;
- Datas e validade das auditorias organizacionais e técnicas mais recentes;
- Datas de incidentes conhecidos e status de correção.

5.2 AST-CLASS Regras para classificação e rotulagem dos dados

5.2.1 AST-CLASS-1 O(s) Departamento(s) responsável(is) pela Segurança da Informação definirá um quadro para classificar os dados de acordo com a sua sensibilidade e regulamentação aplicável, em especial as relativas à proteção de dados pessoais.

5.2.2 AST-CLASS-2 Os Referentes de Segurança da Informação garantem e verificam regularmente se os dados são corretamente classificados e processados pelos Proprietários de Produtos, Gerentes de Produtos e outros usuários de acordo com seu nível de sensibilidade e em conformidade com os regulamentos aplicáveis, particularmente aqueles relativos à proteção de dados pessoais.

5.3 AST-OKUSE Regras para uso aceitável de informações e ativos de hardware e software

5.3.1 AST-OKUSE-1 O(s) Departamento(s) responsável(is) pela Segurança da Informação definirá, implantará, verificará e melhorará continuamente as regras e procedimentos relativos ao uso aceitável da informação, em particular, no que diz respeito à coleta, acesso, processamento, cruzamento, armazenamento, arquivamento, transmissão, publicação e destruição de dados de acordo com as necessidades do negócio e a sensibilidade dos dados.

5.3.2 AST-OKUSE-2 Os Referentes de Segurança da Informação devem documentar e comunicar claramente aos utilizadores legítimos as regras e procedimentos que regem a utilização dos dados, e verificar a sua correta utilização, de acordo com os processos de cibersegurança dos dados.

5.3.3 AST-OKUSE-3 O(s) Departamento(s) responsável(is) pelas Infraestruturas de SI ou OT definem, implementam, verificam e melhoram continuamente as regras e procedimentos relativos à utilização aceitável de dispositivos que possam afetar a segurança dos sistemas de informação do Grupo de Serviços Financeiros da Mobilize, em particular, endpoints, servidores, redes com ou sem fios, caixas de correio e suportes de armazenamento externos (chave USB, disco rígido externo, etc.).

5.3.4 AST-OKUSE-4 O(s) departamento(s) responsável(is) pelas Infraestruturas de SI ou OT devem fornecer aos utilizadores legítimos as regras e procedimentos que regem a utilização de dispositivos que possam afetar a segurança dos sistemas de informação do Grupo de Serviços Financeiros da Mobilize, incluindo procedimentos de acesso, devolução e eliminação, e verificar a sua correta utilização.

5.3.5 AST-OKUSE-5 O Product Owner, com o apoio do Product Manager, deve definir, implantar, verificar e melhorar continuamente as regras e procedimentos relativos ao uso aceitável dos Produtos com Elementos Digitais.

A implantação deve envolver, por exemplo, a distribuição de um manual do usuário para os usuários do produto.

Principle 6 Garantindo acesso Seguro aos ativos

6.1 ACC-Regras Usuárias para o acesso do usuário

6.1.1 ACC-USERS-1 O(s) departamento(s) responsável(is) pela Gestão do Acesso à Identidade definirá, implantará, verificará e melhorará o diretório central de usuários com identificador pessoal padronizado para cada usuário físico (interno ou externo).

6.1.2 ACC-USERS-2 O(s) departamento(s) responsável(is) pelo Gerenciamento de Acesso a Identidades deve definir, implantar, verificar e melhorar a política de gerenciamento de senhas.

6.1.3 ACC-USERS-3 O(s) departamento(s) responsável(is) pela Gestão do Acesso à Identidade, com o apoio do(s) Departamento(s) responsável(is) pela Cibersegurança, definirá, implementará, verificará e melhorará regras, processos e soluções técnicas para o acesso dos utilizadores à rede do Mobilize Financial Services Group (com fios ou Wi-Fi), às redes restritas e às aplicações do Mobilize Financial Services Group, especificando métodos de ligação (por exemplo, login/palavra-passe, autenticação multifator, fator físico...) e equipamentos autorizados, dependendo da criticidade das redes ou aplicações e da sensibilidade dos dados.

6.1.4 ACC-USERS-4 O(s) departamento(s) responsável(is) pela Gestão do Acesso à Identidade autorizará o acesso apenas à Rede do Grupo de Serviços Financeiros Mobilize para execução dos Serviços Financeiros e ao pessoal externo no contexto de um serviço contratualmente acordado que exija esse acesso, com equipamento que cumpra as regras definidas.

6.1.5 ACC-USERS-5 O(s) departamento(s) responsável(is) pelas infraestruturas de SI ou OT devem criar e proteger a rede do Grupo de Serviços Financeiros Mobilize e, se necessário, redes restritas específicas.

6.1.6 ACC-USERS-6 O(s) departamento(s) responsável(is) pelas Infraestruturas de SI ou OT definem, implementam, verificam e melhoram as regras, processos e soluções para aceder à rede do grupo Mobilize Financial Services a partir do exterior, necessariamente através de uma Rede Privada Virtual.

6.1.7 ACC-USERS-7 O(s) departamento(s) responsável(is) pela Gestão do Acesso à Identidade deve criar e manter o registo dos direitos e acessos concedidos para garantir a rastreabilidade das ações realizadas na Rede de Serviços Financeiros Mobilize e em redes restritas específicas.

6.1.8 ACC-USERS-8 O(s) departamento(s) responsável(is) pelas Infraestruturas de SI devem criar e proteger, para cada local, Redes de Convidados isoladas das outras Redes do Grupo de Serviços Financeiros Mobilize para ligar os dispositivos dos visitantes.

6.1.9 ACC-USERS-9 O(s) departamento(s) responsável(is) pela Gestão do Acesso à Identidade deve estabelecer e manter o registo dos direitos e acessos concedidos para garantir a rastreabilidade das ações realizadas nas Redes de Convidados.

6.2 ACC-ADMIN Regras para usuários com acesso privilegiado

6.2.1 ACC-ADMIN-1 O(s) departamento(s) responsável(is) pelas Infraestruturas de SI ou OT devem definir, implementar, verificar e melhorar regras, processos e soluções para acesso privilegiado, uma vez que esse acesso representa um elevado risco para os sistemas de informação do Mobilize Financial Services Group ou dos seus Produtos com Elementos Digitais.

6.3 ACC-TECHN Regras para acesso através de contas de serviço

6.3.1 ACC-TECHN-1 O(s) departamento(s) encarregado(s) do Gerenciamento de Acesso a Identidades também gerenciará contas de serviço com identificador padronizado no diretório central de usuários e definirá, implantará, verificará e melhorará regras e processos para uso seguro de contas de serviço.

6.3.2 ACC-TECHN-2 O(s) Departamento(s) responsável(is) pela Gestão de Acesso à Identidade, com o apoio do(s) Departamento(s) responsável(is) pela Cibersegurança, definirá, implantará, verificará e melhorará regras, processos e soluções técnicas para o acesso técnico aos sistemas ou aplicativos do Mobilize Financial Services Group para minimizar a possibilidade de acesso não autorizado.

Principle 7 Garantir a Segurança Patrimonial

7.1 SEC-PHY Regras para a segurança cibernética física e ambiental

7.1.1 SEC-PHY-1 O(s) departamento(s) responsável(is) pela Segurança Física deve proteger as instalações e os equipamentos físicos (por exemplo, endpoints, servidores, equipamentos de rede e cabeamento) a fim de proteger os dados, de acordo com sua sensibilidade e regulamentos aplicáveis, permitindo que apenas pessoas autorizadas acessem essas instalações, partes das instalações e equipamentos físicos e, seguindo e rastreando esse acesso.

7.1.2 SEC-PHY-2 Ao projetar um Produto de hardware com Elementos Digitais para colocação no mercado (por exemplo, carros), o(s) Departamento(s) responsável(is) pela Engenharia deve definir, implantar, verificar e melhorar continuamente as regras e processos para evitar ataques físicos que possam comprometer o sistema de informação do Produto com Elementos Digitais.

7.2 SEC-CRY Regras de criptografia

7.2.1 SEC-CRY-1 O(s) departamento(s) responsável(is) pela Cibersegurança deve definir, implantar, verificar e melhorar as regras relativas à criptografia e aos processos de uso da criptografia, permitindo que os Product Owners e Product Managers garantam que os dados estejam seguros, de acordo com seu nível de sensibilidade, e reduzam o risco de uso incorreto ou inadequado.

7.3 SEC-DEV Regras para a cibersegurança do ciclo de vida do desenvolvimento

7.3.1 SEC-DEV-1 O(s) departamento(s) responsável(is) pela Cibersegurança deve definir, implantar, verificar e melhorar regras e processos para o ciclo de vida de desenvolvimento seguro, incluindo separação de ambientes de desenvolvimento, teste e produção, orientação para segurança cibernética no desenvolvimento de software, requisitos de segurança cibernética na fase de especificação e projeto, modelagem de ameaças, marcos de segurança cibernética, testes de sistema e segurança cibernética, repositórios seguros para código-fonte e configuração e segurança cibernética na versão Controle.

7.3.2 SEC-DEV-2 O(s) departamento(s) responsável(is) pela Segurança Cibernética deve garantir que os desenvolvedores sejam treinados e conheçam regras e processos para um ciclo de vida de desenvolvimento seguro.

7.4 SEC-PURCH Regras para a cibersegurança de aquisição e serviços IS/OT externos

7.4.1 SEC-PURCH-1 O(s) departamento(s) responsável(is) pela Cibersegurança, com o apoio do(s) Departamento(s) responsável(is) pelas Compras e Departamento(s) responsável(is) pelo Jurídico, definirá, implementará, verificará e melhorará as regras e processos para a aquisição de Produtos seguros com Elementos e componentes Digitais, incluindo requisitos de cibersegurança na fase de especificação e concepção, modelação de ameaças, pontos de verificação de cibersegurança, testes de sistemas e cibersegurança, acesso ao código-fonte, configuração e segurança cibernética no controle de versão.

7.4.2 SEC-PURCH-2 O(s) Departamento(s) responsável(is) pelas Compras, com o apoio do(s) Departamento(s) responsável(is) pela Cibersegurança e do(s) Departamento(s) responsável(is) pelo Jurídico, define, implementa, verifica e melhora o processo de gestão da cibersegurança nos contratos com o fornecedor de Nível 1 de Produtos com Elementos Digitais ou componentes com elementos digitais (hardware ou software) e prestadores de serviços de Nível 1 para garantir que os contratos incluam no Apêndice de Segurança Cibernética todos os requisitos de cibersegurança necessários para controlar riscos, nomeadamente:

- Correspondências de classificação de dados, regras de processamento e requisitos de segurança de dados;
- Requisitos de cibersegurança para a infraestrutura de SI do fornecedor/prestador de serviços, com base na sensibilidade dos dados tratados e na necessidade de disponibilidade, integridade, confidencialidade, autenticidade, rastreabilidade e não repúdio;
- Requisitos para o cumprimento de obrigações legais e regulamentares, nomeadamente em termos de cibersegurança, proteção de dados pessoais e legislação em matéria de propriedade intelectual e direitos de autor;
- Requisitos para a caução e transferência de códigos-fonte, para que o Mobilize Financial Services Group possa continuar suas atividades se o fornecedor ou provedor de serviços não puder fazê-lo;
- Detalhamento dos controles, incluindo acesso, desempenho, monitoramento e auditorias;
- Requisitos de conscientização e treinamento;
- Requisitos que o vendedor ou fornecedor de nível 1 deve replicar ao longo de toda a cadeia contratual com os seus vendedores ou fornecedores e informações a fornecer sobre a cadeia de subcontratação;
- Requisitos de gerenciamento de incidentes, incluindo requisitos de notificação, colaboração e compartilhamento de informações;
- Medidas corretivas e sanções e indenizações em caso de descumprimento de requisitos por parte do vendedor ou fornecedor;
- Quando aplicável, as certificações necessárias para o fornecedor ou fornecedor;
- Mobilizar os direitos de auditoria organizacional e técnica do Grupo de Serviços Financeiros, especificando regras de ativação, frequências, prazos e alocação de custos;
- Requisitos relativos à devolução de ativos e à transferência de dados num formato utilizável para garantir a interoperabilidade.

7.4.3 SEC-PURCH-3 O(s) Departamento(s) responsável(is) pelas Compras deve assegurar que o contrato com o Apêndice de Cibersegurança seja assinado antes da entrega dos Produtos com Elementos Digitais ou componentes com elementos digitais ou antes da prestação do serviço IS/OT.

7.4.4 SEC-PURCH-4 O(s) Departamento(s) responsável(is) pelas Compras deve assegurar que seja elaborado e assinado um aditivo ao contrato e ao Apêndice de Cibersegurança antes de qualquer

alteração aos Produtos acordados com Elementos Digitais ou componentes com elementos digitais ou serviço IS/OT.

7.5 SEC-OPEMA Regras para cibersegurança de operação, manutenção e descarte

7.5.1 SEC-OPEMA-1 O(s) departamento(s) responsável(is) pelas infraestruturas de SI ou OT, com o apoio do(s) departamento(s) responsável(is) pela cibersegurança, deve definir, implementar, verificar e melhorar as regras e processos de gestão da cibersegurança da operação, incluindo a gestão do acesso e rastreabilidade, as cópias de segurança, a gestão da capacidade, a manutenção, a gestão de vulnerabilidades técnicas, os procedimentos de reinicialização e recuperação do sistema, a supervisão, a gestão da obsolescência e a eliminação.

7.5.2 SEC-OPEMA-2 O(s) departamento(s) responsável(is) pelas Infraestruturas de SI ou OT, com o apoio do(s) Departamento(s) responsável(is) pela Cibersegurança, devem estabelecer, implementar, verificar e melhorar regras, processos e soluções técnicas para a proteção de ativos contra malware.

7.5.3 SEC-OPEMA-3 O(s) departamento(s) responsável(is) pelas Infraestruturas de SI ou OT, com o apoio do(s) Departamento(s) responsável(is) pela Cibersegurança, define, implementará, verificará e melhorará regras e processos específicos de cibersegurança para operação em ambiente cloud.

7.5.4 SEC-OPEMA-4 O(s) departamento(s) responsável(is) pelas Infraestruturas de SI ou OT devem assegurar o cumprimento das regras e processos de cibersegurança da operação por parte dos Product Owners e Product Managers;.

7.6 SEC-WKSTA Regras para segurança cibernética em estações de trabalho

7.6.1 SEC-WKSTA-1 O(s) departamento(s) responsável(is) pelos Endpoints, com o apoio do(s) Departamento(s) responsável(is) pela Segurança Cibernética e do(s) Departamento(s) responsável(is) pela Segurança Física, define, implantará, verificará e atualizará as regras e processos de segurança cibernética da estação de trabalho, incluindo provisionamento, segurança física, reatribuição de estação de trabalho, gerenciamento de privilégios, proteção de dados e trabalho remoto.

7.7 SEC-REMWK Regras para o trabalho remoto

7.7.1 SEC-REMWK-1 O(s) departamento(s) responsável(is) pelas infraestruturas de SI deve implementar medidas específicas de cibersegurança para controlar os riscos associados ao teletrabalho e fornecer a todos os teletrabalhadores equipamentos seguros adequados.

7.7.2 SEC-REMWK-2 O(s) departamento(s) responsável(is) pelas infraestruturas de SI deve definir e comunicar as obrigações e as melhores práticas a seguir pelos trabalhadores remotos.

7.8 SEC-CLOUD Regras de segurança cibernética para uso de serviços em nuvem

7.8.1 SEC-CLOUD-1 O(s) departamento(s) responsável(is) pelas Infraestruturas de SI, com o apoio do(s) Departamento(s) responsável(is) pela Cibersegurança, define, implementará, verificará e melhorará as regras e processos de cibersegurança para a utilização de serviços em nuvem, incluindo:

- Critérios de seleção de serviços em nuvem;
- Funções e responsabilidades para gerenciar serviços em nuvem;

- Distribuição de controles de segurança cibernética entre o Mobilize Financial Services Group e o provedor de serviços em nuvem;
- Meios de verificação dos controles de segurança cibernética implementados pelos provedores de serviços em nuvem;
- Meios de controlar interações entre diferentes serviços de nuvem e alterações em serviços de nuvem;
- Gerenciamento de riscos de serviços em nuvem;
- Gerenciamento de incidentes de serviços em nuvem;
- Gerenciamento de alterações ou cessação do uso de serviços de nuvem.

7.9 SEC-NETWK Regras para segurança cibernética de rede

7.9.1 SEC-NETWK-1 O(s) departamento(s) responsável(is) pelas infraestruturas de SI ou OT, com o apoio do(s) departamento(s) responsável(is) pela Cibersegurança, define, implementa, verifica e melhora as regras e processos para a cibersegurança da rede do Mobilize Financial Services Group e a cibersegurança das interações entre a rede do Mobilize Financial Services Group e redes de terceiros, incluindo a gestão, configuração, filtragem e particionamento, com o objetivo de proteger os dados em trânsito, dependendo de sua sensibilidade.

7.9.2 SEC-NETWK-2 O(s) Departamento(s) responsável(is) pelo Desenvolvimento de Produto com Elementos Digitais, com o apoio do(s) Departamento(s) responsável(is) pela Cibersegurança, definirá, implementará, verificará e melhorará as regras e processos de cibersegurança das interações entre o produto do Grupo Mobilize Financial Services e os sistemas de informação offboard, incluindo a gestão, configuração, filtragem e particionamento, com o objetivo de proteger os dados em trânsito, dependendo de sua sensibilidade.

7.9.3 SEC-NETWK-3 O(s) departamento(s) responsável(is) pelas infraestruturas de SI, com o apoio do(s) departamento(s) responsável(is) pela Cibersegurança, define, implantará, verificará e melhorará as regras e processos de cibersegurança dos meios de telecomunicações do Mobilize Financial Services Group (por exemplo, telefones, e-mails, etc.).

Principle 8 Garantir a conformidade e a melhoria contínua da cibersegurança

8.1 COM-MONIT Regras para monitoramento, medição e avaliação da conformidade, risco e eficiência de segurança cibernética

8.1.1 COM-MONIT-1 O Proprietário do Processo deve definir e produzir indicadores relevantes a intervalos regulares para permitir que os níveis de conformidade, eficácia e risco relativos aos seus processos sejam monitorizados, medidos e avaliados.

8.1.2 COM-MONIT-2 O Proprietário do Processo deve considerar os alertas levantados pelos clientes do processo sobre a falta de eficiência, conformidade ou um risco relativo ao processo.

8.1.3 COM-MONIT-3 O CISO deve coletar estes indicadores e criar dashboards adequados, atualizados a intervalos regulares, para poder gerir as atividades de cibersegurança e comunicar eficazmente com os vários comités e partes interessadas, incluindo a Equipe de Liderança, sobre a evolução dos níveis globais de eficácia e conformidade dos sistemas de gestão da cibersegurança e a evolução dos riscos que pesam sobre o Mobilize Financial Services Group.

8.2 COM-AUDTE Regras para auditorias técnicas

8.2.1 COM-AUDTE-1 O CISO deve definir a política para avaliações técnicas de cibersegurança e testes de penetração e especificar a sua frequência de acordo com a regulamentação aplicável, o estado da técnica, o tipo de Produto com Elementos Digitais e o nível de criticidade dos Produtos com Elementos Digitais a testar.

8.2.2 COM-AUDTE-2 O CISO decidirá criar, com o apoio do(s) Departamento(s) responsável(is) pela Segurança Física, uma Equipe Vermelha "red team" para testar a cibersegurança técnica dos sistemas de informação do Grupo Mobilize Financial Services dentro de um perímetro definido pelo CISO, com base nos objetivos de cibersegurança e riscos existentes.

8.3 COM-CHECK Regras para verificações de conformidade organizacional

8.3.1 COM-CHECK-1 O CISO deve verificar regularmente se os sistemas de gestão em vigor e os processos operacionais associados são eficazes e cumprem a estratégia, os objetivos e a política de cibersegurança do Mobilize Financial Services Group, os regulamentos internacionais e nacionais e as normas internacionais que o Mobilize Financial Services Group decidiu aplicar, através de avaliações de cibersegurança e auditorias externas.

8.4 COM-AUDIN Regras para auditorias internas

8.4.1 COM-AUDIN-1 O(s) Departamento(s) responsável(is) pelas Auditorias deve criar e implementar periodicamente, com o apoio do CISO e dos Pilotos do Sistema de Gestão da Cibersegurança, e de acordo com a Carta de Auditoria Interna, um programa de auditoria dos Sistemas de Gestão da Cibersegurança, a fim de verificar a conformidade destes sistemas com a Política de Cibersegurança, as regulamentações nacionais e internacionais a que o Mobilize Financial Services Group está sujeito e, quando aplicável, as normas internacionais que o Mobilize Financial Services Group decide aplicar.

8.4.2 COM-AUDIN-2 Qualquer pessoa notificada como responsável pela correção de uma não conformidade identificada pelo(s) departamento(s) responsável(is) pelas auditorias deve cooperar plenamente na definição e implementação das medidas corretivas necessárias.

8.5 COM-AUDPU Regras para auditorias de vendedores e fornecedores

8.5.1 COM-AUDPU-1 O(s) departamento(s) responsável(is) pela Cibersegurança define, implementa, verifica e aprimora as regras e processos para a realização de auditorias organizacionais e técnicas para verificar a eficácia da cibersegurança contratualmente acordada com fornecedores e fornecedores.

8.5.2 COM-AUDPU-2 O(s) departamento(s) responsável(is) pela Cibersegurança deve assegurar que os requisitos relativos às auditorias organizacionais e técnicas estão devidamente integrados no(s) departamento(s) responsável(is) pelos processos de Compras e contratos com fornecedores de Produtos com Elementos Digitais ou componentes com elementos digitais e fornecedores de SI.

8.6 COM-LDRVW Regras para revisões de segurança cibernética da equipe de liderança

8.6.1 COM-LDRVW-1 Todos os anos, a Equipe de Liderança deve rever o nível dos sistemas de gestão da cibersegurança e decidir sobre as novas ações de cibersegurança a adotar para melhorar a postura de cibersegurança do Mobilize Financial Services Group, com base em:

- O progresso das ações decididas em Revisões de Cibersegurança da Equipe de Liderança anteriores e a extensão em que os objetivos foram alcançados;
- A evolução da estratégia global do Mobilize Financial Services Group e os desafios internos e externos;
- Indicadores de desempenho do sistema de gestão de cibersegurança;
- Indicadores de risco de cibersegurança, avaliações de risco e andamento dos planos de tratamento de riscos;
- Resultados de auditoria e andamento de ações para correção de não conformidades;
- Propostas de melhoria contínua apresentadas pelo CISO.

Principle 9 Garantir a gestão de incidentes cibernéticos

9.1 INC-MANAG Regras para gestão de incidentes

9.1.1 INC-MANAG-1 O(s) Departamento(s) responsável(is) pela Cibersegurança definirá, implementará, verificará e melhorará o processo de gestão de incidentes para a comunicação de eventos de cibersegurança, administração, documentação, recolha de provas, detecção, triagem, priorização, análise, comunicação, coordenação das partes interessadas, resposta e capitalização.

9.1.2 INC-MANAG-2 O(s) Departamento(s) responsável(is) pela Cibersegurança deve assegurar que as pessoas que devem contribuir para a gestão de incidentes sejam regularmente treinadas e, se necessário, que essas pessoas possuam as certificações necessárias.

Principle 10 Garantir a continuidade dos negócios e o gerenciamento de crise

10.1 BUS-CONTI Regras para a continuidade de negócios

10.1.1 BUS-CONTI-1 O(s) departamento(s) responsável(is) pela Continuidade de Negócios, com o apoio do(s) Departamento(s) responsável(is) pela Cibersegurança, definirá regras e processos de continuidade de negócios e gestão de crises, de acordo com a criticidade dos processos a serem protegidos e a sensibilidade dos dados para garantir a continuidade das operações e, se isso não for possível, restaurar os sistemas de informação a fim de reiniciar as operações em ordem de prioridade.

10.1.2 BUS-CONTI-2 O(s) departamento(s) responsável(is) pela Continuidade de Negócios assegurará(ão) que:

- São mapeados aplicativos, recursos críticos de negócios e sistemas de informação;
- Gerentes de Produto definiram e testaram Planos de Recuperação de Desastres para seus Produtos com Elementos Digitais;
- É definida, implantada e comunicada uma estrutura de gestão adequada para preparar, mitigar e responder a uma crise;
- Os planos de continuidade de negócios são definidos e comunicados para gerenciar as 4 fases de uma crise:
  - ✓ alertar, mobilizar e conter;
  - ✓ manter a confiança e compreender o ataque;

- ✓ retomada das atividades empresariais e fortalecimento dos sistemas de informação;
- ✓ lições aprendidas e capitalização

- Os exercícios de gestão de crises são realizados regularmente no âmbito do Grupo Mobilize Financial Services, se necessário envolvendo terceiros.

10.1.3 BUS-CONTI-3 Para cobrir a totalidade ou parte das perdas em caso de crise de cibersegurança, o Mobilize Financial Services Group pode contratar um seguro cibernético. Neste caso, o(s) Departamento(s) responsável(is) pela Cibersegurança, com o apoio do(s) Departamento(s) responsável(is) pelo Seguro, estabelecerá as regras e os processos para a contratação e ativação do seguro cibernético.

05 A LISTA DE REGRAS BANCÁRIAS

Princípio 1 Garantir uma governança eficiente da cibersegurança

1.2 GOV-ORGAN Regras para a organização, funções e responsabilidades de segurança cibernética

1.2.10.1 Deve ser aplicado um sistema de controle interno para cumprir os requisitos da regulamentação bancária (Decreto de 3 de novembro de 2014 revisto em 25 de fevereiro de 2021) em 3 níveis:

Controle pela equipe operacional (primeira linha de defesa);
Controle pelo risco e controle interno (segunda linha de defesa);
Controle pela auditoria interna (terceira linha de defesa).

Princípio 3 Garantir a segurança cibernética controlada com base em riscos

3.1 RSK-MANAG Regras para gestão de riscos

3.1.1.1 O CISO de cada entidade deve implementar uma gestão de riscos informáticos baseada na apetência de risco da sua atividade ou setor. Esta metodologia e processo terão de ser continuamente melhorados e adaptados, incluindo as seguintes etapas:

a. Identificação (ativos, ameaças, vulnerabilidades, impacto);
b. Análise (avaliação de impacto e probabilidade de ocorrência);
c. Avaliação;
d. Tratamento.

3.1.1.2 O quadro de gestão de riscos de ICT deve ser documentado e revisto pelo menos uma vez por ano, bem como após a ocorrência de grandes incidentes relacionados com ICT que tenham um elevado impacto adverso na rede e nos sistemas de informação que suportam funções críticas ou importantes do Mobilize Financial Services Group, e seguindo instruções de supervisão ou conclusões derivadas de processos relevantes de auditoria ou testes de resiliência operacional digital. É continuamente melhorado com base em lições derivadas da implementação e monitoramento. A pedido desta, é apresentado à autoridade competente um relatório sobre a revisão do quadro de gestão dos riscos das ICT.

3.1.1.3 O Mobilize Financial Services Group define, no contexto da estratégia de resiliência operacional digital, uma estratégia global de multifornecedores de ICT, a nível de grupo ou entidade, mostrando as principais dependências de prestadores de serviços terceirizados de ICT e explicando a lógica por trás do mix de aquisições de prestadores de serviços terceirizados de ICT.

3.1.1.4 Como parte da gestão de riscos, o Mobilize Financial Services Group:

a. Criar e manter um quadro sólido e documentado de gestão dos riscos das ICT que especifique os mecanismos e as medidas destinados a uma gestão rápida, eficiente e abrangente dos riscos das TIC, nomeadamente para a proteção dos componentes físicos e das infraestruturas relevantes;

b. monitoriza continuamente a segurança e o funcionamento de todos os sistemas de ICT;

c. minimiza o impacto do risco das TIC através da utilização de sistemas, protocolos e ferramentas de ICT sólidos, resilientes e atualizados, adequados para apoiar o desempenho das suas atividades

e a prestação de serviços e proteger adequadamente a disponibilidade, autenticidade, integridade e confidencialidade dos dados na rede e nos sistemas de informação;

d. Permite que as fontes de risco e anomalias das ICT na rede e nos sistemas de informação sejam prontamente identificadas e detectadas e que os incidentes relacionados com as ICT sejam rapidamente tratados;

e. identifica as principais dependências dos prestadores de serviços terceirizados de ICT;

f. Assegura a continuidade de funções críticas ou importantes, através de planos de continuidade das atividades e de medidas de resposta e recuperação, que incluam, pelo menos, medidas de apoio e restauração;

g. Analisa regularmente os planos e medidas referidos na alínea f), bem como a eficácia dos controlos aplicados em conformidade com as alíneas a) e c);

h. Implementa, conforme adequado, as conclusões operacionais relevantes resultantes dos testes e da análise pós-incidente no processo de avaliação dos riscos das ICT e desenvolve, de acordo com as necessidades e o perfil de risco das ICT, programas de sensibilização para a segurança das ICT e formação em resiliência operacional digital para o pessoal e a gestão.

3.1.1.5 Para os propósitos da estrutura de gerenciamento de risco de ICT, o Mobilize Financial Services Group adota uma estratégia de risco de provedor de serviços de ICT de terceiros e a revisa regularmente, levando em conta a estratégia de vários fornecedores. A estratégia de risco para prestadores de serviços de ICT terceiros inclui uma política sobre a utilização de serviços de ICT que suportam funções críticas ou importantes fornecidas por prestadores de serviços de ICT terceiros e aplica-se numa base individual e, numa base subconsolidada e consolidada. Com base numa avaliação do perfil de risco global da entidade financeira e do âmbito e complexidade dos serviços, o órgão de administração analisa regularmente os riscos identificados no que diz respeito aos acordos contratuais para a utilização de serviços de ICT que apoiem funções críticas ou importantes.

Princípio 4 Garantir a integração da segurança cibernética em todos os produtos com elementos digitais

4.1 INT-RESPO Regras de responsabilidade

4.1.2.1 Todas as entidades que processam, armazenam ou transmitem informações de cartões de pagamento devem estar em conformidade com o PCI-DSS (Payment Card Industry - Data Security Standard) e certificadas com o nível adequado de acordo com o volume de transações de cartão de pagamento realizadas anualmente. Isto inclui os prestadores de serviços de pagamento e quaisquer outras entidades envolvidas no tratamento de transações com cartões de pagamento.

4.4 INT-ACQUI Regras para a aquisição de produtos com elementos ou componentes digitais ou o uso de um fornecedor de serviços.

4.4.1.1 As orientações sobre a externalização e a recomendação sobre a externalização para prestadores de serviços em nuvem fornecidas pela EBA (EBA/GL/2019/02) devem ser implementadas, em particular, nos seguintes tópicos:

- Funções críticas e importantes;
- Estrutura de governança e gestão de riscos;
- Política de terceirização (responsabilidades);
- Conflitos de interesse.
- Plano de continuidade de negócios;
- Auditoria interna;

- Documentação;
- Processo de terceirização;
- Fase contratual;
- Controle de funções terceirizadas;
- Estratégias de saída.

4.4.1.2 Serviços terceirizados essenciais implicam implantação e acompanhamento regular. Os critérios e obrigações estão especificados no artigo 37-2 da CRBF 97-02 (e incluídos no decreto de 3 de novembro de 2014), em particular os seguintes pontos importantes:

- Cumprimento legal de contratos;
- Reversibilidade dos contratos;
- Sustentabilidade do fornecedor;
- Proteção de dados confidenciais;
- Risco de concentração;
- Subdelegação;
- Monitoramento e controle de indicadores;
- Cláusula de auditoria do fornecedor;
- Acompanhamento por um único interlocutor.

4.6 INT-OPERT Regras para a Operação

4.6.8.1 O Mobilize Financial Services Group deve realizar regularmente, e pelo menos anualmente, uma avaliação específica dos riscos de ICT em todos os sistemas de TIC antigos e, em qualquer caso, antes e depois de ligar tecnologias, aplicações ou sistemas.

4.7 INT-VLNMG Regras para gerenciamento de vulnerabilidade e conformidade em todo o ciclo de vida do produto com elementos digitais

4.7.1.1 O programa de teste de resiliência operacional digital deve fornecer, para a execução de testes apropriados, como avaliações e varreduras de vulnerabilidade, análises de código aberto, avaliações de segurança de rede, análises de lacunas, revisões de segurança física, questionários e soluções de software de varredura, revisões de código-fonte, quando viável, testes baseados em cenários, testes de compatibilidade, testes de desempenho, testes de ponta a ponta e testes de penetração.

4.7.1.2 O Mobilize Financial Services Group deve realizar avaliações de vulnerabilidade antes de qualquer implantação ou reimplantação de aplicativos e componentes de infraestrutura novos ou existentes, e serviços de ICT que apoiem funções críticas ou importantes da entidade financeira.

4.7.1.3 O Mobilize Financial Services Group realiza testes combinando uma abordagem baseada no risco com o planeamento estratégico dos testes de TIC, tendo devidamente em conta a necessidade de manter uma abordagem equilibrada entre, por um lado, a escala de recursos e o tempo a dedicar aos testes de TIC e, por outro lado, a emergência, o tipo de risco, a criticidade dos ativos de informação e os serviços prestados, e quaisquer outros fatores relevantes, incluindo a capacidade do Mobilize Financial Services Group de assumir riscos calculados.

4.8 INT-CONTI Regras para a continuidade, incidente e gestão de crise

4.8.1.1 O Mobilize Financial Services Group mantém pelo menos um local de processamento secundário dotado de recursos, capacidades, funções e alocação de pessoal adequados para garantir as necessidades de negócios. O local de báscula secundária deve ser:

- situado a uma distância geográfica do local de transformação principal, a fim de assegurar que este ostenta um perfil de risco distinto e de evitar que seja afetado pelo mesmo acontecimento que impactou o local primário;

- capaz de assegurar a continuidade de funções críticas ou importantes idênticas ao local primário, ou fornecer o nível de serviços necessários para assegurar que o Mobilize Financial Services Group execute as suas operações críticas dentro dos objetivos de recuperação;

- imediatamente acessível aos funcionários do Mobilize Financial Services Group para garantir a continuidade de funções críticas ou importantes no caso de o local de processamento primário se tornar indisponível.

4.8.1.2 O Mobilize Financial Services Group determina as metas de tempo de recuperação e pontos de recuperação para cada função, levando em conta a criticidade da função e os potenciais efeitos gerais na eficiência do mercado.

4.8.1.3 O Mobilize Financial Services Group realiza as verificações e reconciliações necessárias para garantir o mais alto nível possível de integridade de dados após um incidente de TIC. Os mesmos controles são realizados ao reconstituir dados de provedores externos.

4.8.2.1 Ao restaurar dados de backup usando sistemas próprios, o Mobilize Financial Services Group usa sistemas de ICT que são física e logicamente segregados do sistema de TIC de origem. Os sistemas de ICT devem ser protegidos de forma segura contra qualquer acesso não autorizado ou corrupção de ICT e permitir o restabelecimento atempado de serviços que utilizem dados e cópias de segurança do sistema, conforme necessário.

Os planos de recuperação devem permitir a recuperação de todas as transações no momento da interrupção, a fim de permitir que o Mobilize Financial Services Group continue a operar com certeza e conclua a liquidação na data prevista.

Além disso, os prestadores de serviços de comunicação de dados devem manter recursos adequados e dispor de instalações de apoio e de restabelecimento, a fim de oferecer e manter os seus serviços em permanência.

4.8.3.1 O Mobilize Financial Services Group configura sistemas de backup que podem ser ativados de acordo com as políticas e procedimentos de backup, bem como procedimentos e métodos de restauração e recuperação. A ativação de sistemas de backup não deve expor a segurança da rede e dos sistemas de informação nem a disponibilidade, autenticidade, integridade ou confidencialidade dos dados. Os ensaios dos procedimentos de salvaguarda e dos procedimentos e métodos de restabelecimento e recuperação devem ser efetuados periodicamente.

4.8.6.1 O Mobilize Financial Services Group tem mecanismos para detectar prontamente atividades anômalas, incluindo problemas de desempenho da rede de TIC e incidentes relacionados às TIC, e para identificar potenciais pontos únicos materiais de falha. Todos os mecanismos de detecção são testados regularmente.

Princípio 5 Garantir o conhecimento e o controle dos ativos

5.1 AST-MANAG Regras para a gestão de ativos

5.1.1.1 O Mobilize Financial Services Group identifica e documenta todos os processos que dependem de prestadores de serviços de Tecnologias da Informação e Comunicação (ICT) terceirizados e identifica interconexões com provedores de serviços de ICT terceirizados que fornecem serviços de apoio a funções críticas ou importantes.

Princípio 6 Garantindo o acesso seguro aos ativos

6.1 ACC-USERS Regras de acesso para os usuários

6.1.2.1 A política de gestão de senhas deve respeitar as recomendações locais mais recentes e especificar, pelo menos, o nível de complexidade e as condições de renovação.

Principle 7 Garantir a segurança dos ativos

7.4 SEC-PURCH Regras de cibersegurança para a aquisição e serviços de TI externos

7.4.1.1 O Mobilize Financial Services Group designa os prestadores de serviços terceirizados de ICT que são críticos para suas atividades, seguindo uma avaliação que leva em conta os seguintes critérios:

- o impacto sistêmico na estabilidade, continuidade ou qualidade da prestação de serviços financeiros, no caso de o prestador de serviços terceirizado de TIC em causa se deparar com uma falha operacional em grande escala na prestação dos seus serviços, tendo em conta o número de entidades financeiras e o valor total dos ativos das entidades financeiras às quais o prestador de serviços terceirizado de TIC em causa presta serviços;

- o caráter sistémico ou a importância das entidades financeiras que dependem do prestador de serviços de TIC terceiro relevante, avaliada de acordo com os seguintes parâmetros:

  - o número de instituições globais sistemicamente importantes (G-SII) ou outras instituições sistemicamente importantes (O-SII) que dependem do respetivo prestador de serviços terceirizado de TIC;
  - a interdependência entre as G-SII ou O-SII referidas na subalínea i) e outras entidades financeiras, incluindo situações em que as G-SII ou O-SII prestam serviços de infraestruturas financeiras a outras entidades financeiras;

- a confiança das entidades financeiras nos serviços prestados pelo prestador de serviços terceiro de ICT relevante em relação a funções críticas ou importantes de entidades financeiras que, em última análise, envolvam o mesmo prestador de serviços de ICT, independentemente das entidades financeiras dependerem desses serviços direta ou indiretamente, através de acordos de subcontratação;

- o grau de substituibilidade do prestador de serviços terceirizado de TIC, tendo em conta os seguintes parâmetros:

  - a falta de alternativas reais, mesmo parciais, devido ao número limitado de prestadores de serviços terceirizados de ICT ativos em um mercado específico, ou à participação de mercado do prestador de serviços terceirizado de ICT relevante, ou à complexidade ou sofisticação técnica envolvida, inclusive em relação a qualquer tecnologia proprietária, ou às características específicas da organização ou atividade do prestador de serviços terceirizado de ICT;
  - ii) dificuldades relacionadas com a migração parcial ou total dos dados e cargas de trabalho relevantes do prestador de serviços terceirizado de TIC relevante para outro prestador de serviços terceirizado de ICT, devido a custos financeiros significativos, tempo ou outros recursos que o processo de migração pode acarretar, ou ao aumento do risco de ICT ou a outros riscos operacionais aos quais a entidade financeira pode estar exposta por meio dessa migração.

7.4.2.1 Para os fins e finalidades do quadro de gestão de riscos de ICT, o Mobilize Financial Services Group mantém e atualiza, a nível da entidade, subconsolidado e consolidado, um registo

de informação relacionada com todas as disposições contratuais para a utilização de serviços de ICT prestados por terceiros prestadores de serviços de TIC.

Todos os acordos contratuais estão devidamente documentados, distinguindo entre os que abrangem serviços de ICT que suportam funções críticas e os que não o fazem.

Pelo menos uma vez por ano, o Mobilize Financial Services Group comunica às autoridades competentes o número de novos acordos relacionados com a utilização de serviços de ICT, as categorias de prestadores de serviços de ICT de terceiros, o tipo de acordos contratuais e os serviços e funções de ICT prestados.

O Mobilize Financial Services Group coloca à disposição da autoridade competente, mediante solicitação, o registro completo de informações ou seções específicas do registro, e qualquer outra informação considerada necessária para garantir a supervisão eficaz do Mobilize Financial Services Group.

O Mobilize Financial Services Group informa a autoridade competente de qualquer projeto de acordo contratual relativo à utilização de serviços de ICT que apoiem funções críticas ou importantes, bem como quando uma função se tenha tornado crítica ou importante.

7.4.2.2 O Mobilize Financial Services Group garante que os acordos contratuais relacionados com a utilização de serviços de ICT podem ser rescindidos em qualquer uma das seguintes circunstâncias:

- O terceiro prestador de serviços de ICT violou gravemente os requisitos legislativos, regulamentares ou contratuais aplicáveis;

- O acompanhamento dos riscos associados a terceiros prestadores de serviços de ICT revelou a existência de circunstâncias suscetíveis de alterar o desempenho das funções previstas no acordo contratual, incluindo alterações significativas que afetam o acordo ou a situação do terceiro prestador de serviços de ICT;

- O prestador de serviços de TIC de terceiros demonstrou insuficiências na sua gestão global dos riscos de ICT e, em particular, na forma como garante a disponibilidade, autenticidade, integridade e confidencialidade dos dados, sejam eles pessoais ou sensíveis, ou não pessoais;

- A autoridade competente já não pode supervisionar eficazmente o Mobilize Financial Services Group devido aos termos do acordo contratual em questão ou às circunstâncias a ele associadas.

7.4.2.3 Para serviços de ICT que suportam funções críticas ou importantes, o Mobilize Financial Services Group implementa estratégias de saída. As estratégias de saída têm em conta os riscos que podem ocorrer no caso de terceiros prestadores de serviços de ICT, em especial uma eventual falha da sua parte, uma deterioração da qualidade dos serviços de TIC prestados, qualquer perturbação das atividades devido a uma prestação inadequada ou falhada de serviços de ICT ou qualquer risco significativo resultante da continuação da implantação adequada do serviço de TIC em causa, ou a rescisão de acordos contratuais com um terceiro prestador de serviços de TIC em qualquer das circunstâncias listadas acima.

O Mobilize Financial Services Group garante sua capacidade de se retirar de acordos contratuais sem:

- Interromper suas atividades;
- Restringir o cumprimento dos requisitos regulamentares;
- Afetar a continuidade e a qualidade dos serviços prestados aos clientes.

Os planos de saída são completos, documentados, adequadamente testados e periodicamente revisados.

O Mobilize Financial Services Group define soluções alternativas e planos de transição que lhes permitem remover os serviços de ICT e os dados relevantes detidos pelo prestador de serviços de ICT de terceiros e transferi-los de forma segura e integral para fornecedores alternativos ou reintegrá-los internamente.

O Mobilize Financial Services Group tem as medidas de emergência necessárias em vigor para manter a continuidade dos negócios no caso das circunstâncias listadas acima.

7.4.2.4 Sempre que os acordos contratuais relacionados com a utilização de serviços de TIC que suportem funções críticas ou importantes permitam a possibilidade de um terceiro prestador de serviços de TIC subcontratar serviços de ICT que apoiem uma função crítica ou importante a outros prestadores de serviços de ICT terceiros, o Mobilize Financial Services Group avalia as vantagens e os riscos que podem resultar dessa subcontratação, em especial no caso de um subcontratante de serviços de ICT estabelecido num país terceiro.

Quando os acordos contratuais envolvem serviços de ICT que suportam funções críticas ou importantes, o Mobilize Financial Services Group tem em conta a legislação de insolvência que seria aplicável em caso de falência do terceiro prestador de serviços de ICT, bem como quaisquer restrições que possam resultar em caso de recuperação de emergência dos dados do Mobilize Financial Services Group.

Sempre que sejam celebrados acordos contratuais para a utilização de serviços de ICT que apoiem funções críticas ou importantes com um terceiro prestador de serviços de ICT estabelecido num país terceiro, o Mobilize Financial Services Group tem em conta, para além das considerações acima enumeradas, o cumprimento das regras da UE em matéria de proteção de dados e a aplicação efetiva da legislação nesse país terceiro.

Sempre que os acordos contratuais para a utilização de serviços de ICT que suportam funções críticas ou importantes prevejam a subcontratação, o Mobilize Financial Services Group avalia se e como as cadeias de subcontratação potencialmente longas ou complexas são suscetíveis de comprometer a sua capacidade de assegurar um acompanhamento rigoroso das funções abrangidas pelo contrato e a capacidade da autoridade competente para monitorizar eficazmente o Mobilize Financial Services Group nesta matéria.

7.4.2.5 Os acordos contratuais para a utilização de serviços de ICT devem incluir, pelo menos, os seguintes elementos:

- Uma descrição clara e exaustiva de todos os serviços e funções de ICT a prestar pelo terceiro prestador de serviços de ICT, indicando se é permitida a subcontratação de um serviço de ICT que suporte uma função crítica ou importante, ou partes significativas da mesma, e, em caso afirmativo, as condições aplicáveis a essa subcontratação;

- Os locais, em particular as regiões ou países, onde serão prestados os serviços e funções de ICT abrangidos pelo contrato ou pela externalização e onde os dados serão tratados, incluindo o local de armazenamento, e a obrigação de o terceiro prestador de serviços de ICT informar previamente a entidade financeira se tenciona alterar esses locais;

- Requisitos para a disponibilidade, autenticidade, integridade e confidencialidade da proteção de dados, incluindo dados pessoais;

- Disposições relativas à garantia de acesso, recuperação e devolução, num formato facilmente acessível, dos dados pessoais e outros tratados pela entidade financeira em caso de insolvência, resolução, cessação de atividades do terceiro prestador de serviços de ICT ou cessação de acordos contratuais;

- Descrições de nível de serviço, incluindo atualizações e revisões;

- A obrigação de o terceiro prestador de serviços de ICT prestar assistência à entidade financeira, sem custos adicionais ou a um custo pré-determinado, em caso de incidente relacionado com as ICT relacionado com o serviço de ICT prestado ao Mobilize Financial Services Group;

- A obrigação de o terceiro prestador de serviços de ICT cooperar com as autoridades competentes e as autoridades de resolução do Mobilize Financial Services Group, incluindo os seus nomeados;

- Direitos de rescisão e prazos mínimos de pré-aviso para a cessação de acordos contratuais, em consonância com as expectativas das autoridades competentes e das autoridades de resolução;

- Condições para a participação de prestadores de serviços de ICT terceirizados em programas de conscientização de segurança de ICT e treinamento de resiliência operacional digital desenvolvido pelo Mobilize Financial Services Group.

7.4.2.6 Os acordos contratuais para a utilização de serviços de ICT que suportam funções críticas ou importantes incluem, pelo menos, os seguintes elementos, para além dos listados acima:

a. Descrições completas dos níveis de serviço, incluindo atualizações e revisões, com metas de desempenho quantitativas e qualitativas precisas dentro dos níveis de serviço acordados, para permitir o monitoramento eficaz dos serviços de TIC pelo Mobilize Financial Services Group e tomar as medidas corretivas apropriadas sem demora injustificada quando os níveis de serviço acordados não forem atingidos;

b. Períodos de pré-aviso e obrigações de notificação do terceiro prestador de serviços de TIC à Mobilize Financial Services Group, incluindo a notificação de quaisquer desenvolvimentos que possam ter um impacto significativo na capacidade do terceiro prestador de serviços de TIC para fornecer serviços de TIC que suportem funções críticas ou importantes de forma eficaz, de acordo com os níveis de serviço acordados;

c. A obrigação de o terceiro prestador de serviços de TIC implementar e testar planos de emergência e de implementar medidas, ferramentas e políticas de segurança das ICT que proporcionem um nível adequado de segurança para os serviços prestados pelo Mobilize Financial Services Group, em conformidade com o seu quadro regulamentar;

d. A obrigação de o terceiro prestador de serviços de TIC participar e cooperar nos testes baseados em ameaças realizados pelo Mobilize Financial Services Group;

e. O direito de monitorizar continuamente o desempenho do prestador de serviços de ICT de terceiros, que inclui os seguintes elementos:

- Direitos ilimitados de acesso, inspeção e auditoria pelo Mobilize Financial Services Group ou por um terceiro designado, e pela autoridade competente, e o direito de tirar cópias de documentos relevantes no local, se forem essenciais para as atividades do terceiro prestador de serviços de TIC, cujo exercício efetivo não seja impedido ou limitado por outros acordos contratuais ou políticas de execução;
- o direito de acordar outros níveis de garantia se os direitos de outros clientes forem afetados;
- a obrigação de o terceiro prestador de serviços de TIC cooperar com inspeções e auditorias no local realizadas pelas autoridades competentes, pelo supervisor principal, pelo Mobilize Financial Services Group ou por um terceiro designado; e
- a obrigação de fornecer informações pormenorizadas sobre o âmbito, os procedimentos e a frequência dessas inspeções e auditorias;

f. Estratégias de saída, em especial a fixação de um período de transição obrigatório adequado:

- durante o qual o terceiro prestador de serviços de TIC continuará a fornecer as funções ou serviços de TIC relevantes, a fim de reduzir o risco de perturbação do Mobilize Financial Services Group ou de assegurar a sua efetiva resolução e reestruturação;
- que permite ao Mobilize Financial Services Group migrar para outro prestador de serviços de TIC terceirizado ou utilizar soluções internas adaptadas à complexidade do serviço prestado.

Em derrogação (referente ao item e), o terceiro prestador de serviços de ICT e a entidade financeira que é uma microempresa podem acordar que os direitos de acesso, inspeção e auditoria da entidade financeira podem ser delegados num terceiro independente, nomeado pelo terceiro prestador de serviços de ICT e que a entidade financeira tem o direito de solicitar ao terceiro, a qualquer momento, informações e garantias relativas ao desempenho do Terceiro Prestador de Serviços de ICT.

7.4.3.1 O Mobilize Financial Services Group só pode celebrar acordos contratuais com prestadores de serviços terceirizados de ICT que cumpram os padrões apropriados de segurança da informação. Sempre que esses acordos contratuais digam respeito a funções críticas ou importantes, o Mobilize Financial Services Group deve, antes de celebrar os acordos, ter devidamente em conta a utilização, por parte dos prestadores de serviços terceiros no domínio das ICT, dos mais elevados e atualizados padrões de segurança da informação.

Principio 8 Garantir a conformidade e a melhoria contínua da cibersegurança

8.2 COM-AUDTE Regras para as auditorias técnicas

8.2.2.1 Os provedores de equipes vermelhas devem cumprir rigorosamente os requisitos de Equipe Ética Baseada em Inteligência de Ameaças (TIBER-EU). O quadro TIBER-UE explica as principais fases, atividades, resultados e interações que devem ser incluídos num teste TIBER-UE.

8.2.2.2 O Mobilize Financial Services Group realiza testes avançados de intrusão baseados em ameaças pelo menos a cada três anos. Dependendo do perfil de risco e das circunstâncias operacionais, a autoridade competente pode solicitar a redução ou o aumento dessa frequência.

8.2.2.3 Cada teste de intrusão baseado em ameaças abrange várias, se não todas, as funções críticas ou importantes de um Mobilize Financial Services Group são executadas em sistemas em ambientes de produção ao vivo que suportam essas funções.

O Mobilize Financial Services Group identifica todos os sistemas, processos e tecnologias de ICT subjacentes relevantes que suportam funções críticas ou importantes e serviços de TIC, incluindo aqueles que suportam funções críticas ou importantes que foram terceirizados ou subcontratados a prestadores de serviços de ICT terceirizados.

O Mobilize Financial Service avalia quais funções críticas ou importantes devem ser cobertas por testes de intrusão baseados em ameaças. O resultado desta avaliação determina o âmbito preciso destes ensaios e é validado pelas autoridades competentes.

8.2.2.4 Quando prestadores de serviços de ICT terceirizados são incluídos no escopo do teste de penetração baseado em ameaças, o Mobilize Financial Services Group toma as medidas e precauções necessárias para garantir a participação desses provedores de serviços de ICT terceirizados no teste e sempre permanece responsável por garantir a conformidade com a regulamentação DORA.

8.2.2.5 sempre que se possa razoavelmente esperar que a participação de um terceiro prestador de serviços de ICT em testes de intrusão baseados em ameaças afete negativamente a qualidade ou a segurança dos serviços que o terceiro prestador de serviços de ICT fornece a

clientes que são entidades fora do âmbito de aplicação, ou a confidencialidade dos dados relacionados com esses serviços, o Mobilize Financial Services Group e o Prestador de Serviços de ICT de Terceiros podem acordar por escrito que o Prestador de Serviços de ICT de Terceiros celebre diretamente acordos contratuais com um testador externo, com a finalidade de realizar, sob a direção do Mobilize Financial Services Group, um teste de grupo de intrusão baseado em ameaças envolvendo várias entidades financeiras (Group Test) às quais o Terceiro Prestador de Serviços de ICT presta serviços de ICT.

Este teste de grupo abrange a gama relevante de serviços de ICT que suportam funções críticas ou importantes subcontratadas pelo Mobilize Financial Services Group ao prestador de serviços de TIC terceirizado relevante. O teste de grupo é considerado um teste de penetração baseado em ameaças realizado pelas entidades financeiras que participam no teste de grupo.

O número de entidades financeiras que participam no teste de grupo é devidamente calibrado para a complexidade e os tipos de serviços envolvidos.

8.2.2.6 Com a cooperação de prestadores de serviços de ICT terceirizados e outras partes interessadas, incluindo testadores, o Mobilize Financial Services Group realiza controles eficazes de gerenciamento de risco para mitigar os riscos de potencial impacto de dados, danos a ativos e interrupção de funções, serviços ou operações críticas ou importantes dentro do próprio Mobilize Financial Services Group, suas contrapartes ou o setor financeiro.

8.2.2.7 No final do ensaio, uma vez aprovados os relatórios e os planos de ação corretiva, o Mobilize Financial Services Group e, se aplicável, os testadores externos fornecem à autoridade designada um resumo das conclusões relevantes, dos planos de ação corretiva e da documentação que demonstra que o ensaio de penetração baseado em ameaças foi realizado em conformidade com os requisitos.

8.2.2.8 Para realizar testes de intrusão baseados em ameaças, o Mobilize Financial Services Group usa apenas testadores que:

- - Ter e demonstrar as mais altas habilidades e reputação;
- - Ter habilidades técnicas e organizacionais e conhecimentos específicos em inteligência e conhecimento de ameaças, testes de penetração e testes de equipe vermelha;
- - Sejam certificados por um organismo de acreditação num Estado-Membro, ou aderem a códigos formais de conduta ou quadros éticos;
- - Fornecer verificação independente ou um relatório de auditoria demonstrando um bom nível de gerenciamento de riscos relacionados à execução de testes de penetração baseados em ameaças, incluindo a proteção adequada dos riscos operacionais do Mobilize Financial Services Group;
- - Estejam devida e integralmente cobertos pelo seguro de indenização profissional pertinente, inclusive contra os riscos de má conduta e negligência.

8.2.2.9 Ao usar testadores internos, o Mobilize Financial Services Group garante que, além dos requisitos listados acima, as seguintes condições sejam atendidas:

- - A utilização de testadores internos tenha sido aprovada pela autoridade competente relevante ou pela autoridade pública única designada;
- - A autoridade competente em causa verificou que o Mobilize Financial Services Group dispõe de recursos suficientes e tomou as medidas necessárias para evitar conflitos de interesses durante as fases de conceção e execução do teste; e
- - O provedor de inteligência de ameaças é externo ao Mobilize Financial Services Group.

8.2.2.10 O Mobilize Financial Services Group garante que os contratos com testadores externos exijam um gerenciamento eficaz dos resultados dos testes de penetração baseados em ameaças e que o processamento de dados correspondente, incluindo geração, armazenamento, agregação, elaboração, elaboração, relatórios, comunicação ou destruição, não coloque o Mobilize Financial Services Group em risco.

8.4 COM-AUDIN Regras para as auditorias internas

8.4.1.1 O Mobilize Financial Services Group está sujeito a auditorias internas regulares realizadas por auditores de acordo com o plano de auditoria do Mobilize Financial Services Group.

Estes auditores são qualificados e possuem conhecimentos, competências e experiência suficientes na gestão de riscos relacionados com as Tecnologias de Informação e Comunicação (ICT) e demonstram uma independência adequada durante as auditorias. A frequência das auditorias internas é definida no plano de auditoria.

8.4.2.1 A frequência das auditorias internas, os resultados e os planos de ação são definidos no plano de auditoria. Um processo formal de acompanhamento é documentado e sistematicamente aplicado para garantir a correção dos resultados da auditoria.

Principio 9 Garantir a gestão de incidentes cibernéticos

9.1 INC-MANAG Regras para a gestão de incidentes

9.1.1.1 Os mecanismos de detecção permitem várias camadas de controle, definem limites e critérios de alerta para acionar e iniciar processos de resposta a incidentes relacionados às ICT, incluindo mecanismos de alerta automático para funcionários relevantes responsáveis pela resposta a incidentes relacionados às ICT.

9.1.1.2 O Mobilize Financial Services Group usa um processo e uma ferramenta dedicados para relatar a ocorrência de um incidente de segurança. Esses mecanismos garantem a completude dos relatórios de transações, identificam omissões e erros e solicitam a retransmissão desses relatórios.

9.1.1.3 O Mobilize Financial Services Group classifica incidentes relacionados a TIC e determina seu impacto com base nos seguintes critérios:

- - O número e/ou a relevância dos clientes ou das contrapartes financeiras afetados e, se aplicável, o montante ou o número de transações afetadas pelo incidente relacionado com as TIC e se o incidente relacionado com as TIC causou impacto na reputação;
- - a duração do incidente relacionado com as TIC, incluindo o tempo de paragem do serviço;
- - a dispersão geográfica das zonas afectadas pelo incidente relacionado com as TIC, em especial se afectar mais de dois Estados-Membros;
- - as perdas de dados que o incidente relacionado com as TIC acarreta, em relação à disponibilidade, autenticidade, integridade ou confidencialidade dos dados;
- - a criticidade dos serviços afetados, incluindo as transações e operações do Mobilize Financial Services Group;
- - o impacto económico, em especial os custos e perdas directos e indirectos, do incidente relacionado com as TIC, tanto em termos absolutos como relativos.

9.1.1.4 O Mobilize Financial Services Group classifica as ameaças cibernéticas como significativas com base na criticidade dos serviços em risco, incluindo as transações e operações

do Mobilize Financial Services Group, o número e/ou a relevância dos clientes ou contrapartes financeiras visados e a dispersão geográfica das áreas em risco.

9.1.1.5 O Mobilize Financial Services Group comunica os principais incidentes de TIC à autoridade competente relevante.

O Mobilize Financial Services Group designou o BCE como a autoridade competente relevante responsável pelo exercício das funções e deveres.

Após a recolha e análise de todas as informações relevantes, é apresentada uma notificação inicial e um relatório à autoridade competente.

Se for tecnicamente impossível apresentar a notificação inicial utilizando o modelo, é definida outra forma de submeter a notificação inicial à autoridade competente.

A notificação inicial e os relatórios incluem todas as informações necessárias para permitir à autoridade competente determinar a extensão do grave incidente de TIC e avaliar quaisquer implicações transfronteiriças.

9.1.1.6 Quando um incidente de grande impacto de ICT ocorre e afeta os clientes, a Mobilize Financial Services Group informa os clientes afetados pelo incidente de ICT e as medidas que foram tomadas para mitigar os efeitos do incidente sem demora indevida e assim que o Mobilize Financial Services Group tomar conhecimento do incidente.

No caso de uma grande ameaça cibernética, o Mobilize Financial Services Group informa seus clientes potencialmente afetados sobre quaisquer medidas de proteção apropriadas a serem tomadas.

9.1.1.7 A Mobilize Financial Services Group define os prazos para relatar um incidente de ICT:

- - Uma notificação inicial;
- - Um relatório intercalar após a notificação inicial, logo que a situação do incidente inicial tenha mudado significativamente ou a gestão do incidente grave de TIC tenha mudado devido às novas informações disponíveis ou sempre que esteja disponível uma atualização relevante da situação, bem como mediante pedido específico da autoridade competente;
- - Um relatório final, quando a análise de causa raiz estiver concluída, se as medidas de mitigação já foram implementadas ou não, e quando os números de impacto reais estiverem disponíveis em vez de estimativas.

9.1.1.8 De acordo com a legislação setorial nacional, a Mobilize Financial Services Group utiliza serviços de terceirização para as obrigações de relatório e permanece responsável pelo cumprimento dos requisitos de notificação de incidentes.

Principle 10 Garantir a continuidade dos negócios e o gerenciamento de crises

10.1 BUS-CONTI Regras para a continuidade de negócio

10.1.1.1 O plano de contingência e continuidade de negócios (BCP/BRP) deve atender aos requisitos regulatórios locais para a implementação de BCPs/BRPs

10.1.1.2 Como parte da política geral de continuidade de negócios, as entidades financeiras devem realizar uma análise de impacto nos negócios (BIA) de suas exposições a interrupções graves dos negócios. No âmbito da BIA, as entidades financeiras devem avaliar o impacto potencial de perturbações graves dos negócios através de critérios quantitativos e qualitativos, utilizando dados internos e externos e análise de cenários, conforme adequado. A BIA deve considerar a criticidade das funções de negócios identificadas e mapeadas, dos processos de suporte, das

dependências de terceiros e dos ativos de informação e suas interdependências. As entidades financeiras devem assegurar que os ativos e serviços de TIC sejam concebidos e utilizados em total alinhamento com a BIA, em especial no que diz respeito a assegurar adequadamente a redundância de todas as componentes críticas.

10.1.1.3 Ao executar o programa de teste de resiliência operacional digital, a Mobilize Financial Services adota uma abordagem baseada em risco, levando em consideração a evolução do risco de TIC, quaisquer riscos específicos aos quais ele esteja ou possa estar exposto, a criticidade dos ativos de informação e serviços prestados e quaisquer outros fatores que o Mobilize Financial Services Group considere apropriados.

10.1.1.4 A Mobilize Financial Services Group define procedimentos e estratégias para priorizar, classificar e resolver todos os problemas identificados durante os testes e desenvolver métodos internos de validação para garantir que quaisquer fraquezas, falhas ou discrepâncias identificadas sejam totalmente corrigidas.

10.1.1.5 A Mobilize Financial Services Group garante que todos os sistemas e aplicativos de ICT que suportam funções críticas ou importantes sejam submetidos a testes apropriados pelo menos uma vez por ano.

10.1.2.1 Um DRP (Disaster Recovery Plans, plano de recuperação de desastres) deve ser implementado para todos os aplicativos para garantir a consistência e minimizar os riscos:

- DRP em 4 horas (RTO) para aplicações financeiras, 0 perda de dados (RPO) (para França e Corporate)

- DRP em 48h (RTO) para todas as aplicações, 0 perda de dados (RPO) (para França e Corporate)

10.1.2.2 Os testes DRP são implementados pelo menos uma vez por ano. Este requisito deve também ser integrado pelos prestadores de serviços e subcontratantes.

10.1.2.3 A Mobilize Financial Services Group mantém um registro acessível das atividades antes e durante as interrupções quando seus planos de continuidade de negócios, resposta e recuperação são ativados.

10.1.2.4 A Mobilize Financial Services Group fornece às autoridades competentes cópias dos resultados de testes de continuidade de negócios ou exercícios semelhantes.

10.1.2.5 A Mobilize Financial Services Group fornece às autoridades competentes, mediante solicitação, uma estimativa dos custos e perdas anuais causados por grandes incidentes de ICT.

06 REGULAMENTOS E LEIS LOCAIS: EXEMPLOS DE ESPECIFICAÇÕES REGULATÓRIAS LOCAIS

Country	Regulation / Law name and reference	High level description	Application date
Argentina	**Communication "A" 7724: Minimum requirements for the management and control of Information Technology and Security Risks – BCRA (Argentina's Central Bank)**	Exige que as entidades financeiras alinhem a sua estratégia de TI e segurança de acordo com os riscos identificados, com foco na cibersegurança, recuperação de desastres e ciberataques, fornecedores de serviços de TI, técnicas de gestão e proteção de software e hardware, para a sua monitorização e controlo.	10/09/2023
Argentina	**Guidelines for Risk Management in Financial Entities – BCRA (Argentina's Central Bank)**	Estabelece uma estrutura para a gestão de riscos a ser cumprida pelas entidades financeiras na Argentina, definindo tarefas e acompanhamentos a serem realizados em relação à identificação e avaliação de riscos, gerenciamento de riscos, supervisão e monitoramento e comunicação de riscos aos principais diretores da entidade.	25/11/2021
Argentina	**Communication "A" 7266 : Guidelines for cyberincident response and recovery - BCRA (Argentina's Central Bank)**	As diretrizes estabelecem o quadro que as instituições financeiras devem ter em vigor para responder a ataques de cibersegurança e, assim, definem um processo de preparação, resposta e recuperação de ciberataques, incluindo planos, equipamentos e testes.	16/04/2021
Argentina	**Communication "A" 6375 : Expansion of financial entities" and "Minimum requirements for management, implementation and control of risks related to information technology, information systems and associated resources for financial entities – BCRA (Argentina's Central Bank)**	O regulamento estabelece as diretrizes e o quadro que toda entidade financeira na Argentina deve ter sobre a forma como deve realizar a descentralização e terceirização de atividades, por meio da avaliação de riscos associados aos fornecedores de serviços de TI e SI, avaliações periódicas, monitoramento e controle sobre as atividades delegadas aos fornecedores de TI e SI.	17/11/2017
Argentina	**Communication "A" 4609: (Minimum requirements for management, implementation and control of risks related to information technology and information systems) – BCRA (Argentina's Central Bank)**	Exige que as instituições financeiras implementem controles técnicos, administrativos e físicos, bem como realizem avaliações periódicas da eficácia dos controles sobre ativos, sistemas de TI e seu conjunto relacionado. Foi o antecessor da regulamentação 7724 do Banco Central da Argentina.	01/07/2007

Brazil	**Resolution CMN No. 4,557/17**	Estabelece a estrutura de gerenciamento de riscos, incluindo os relacionados à segurança da informação.	01/03/2017
Brazil	**Resolution CMN No. 4,893/21**	Aborda a política de cibersegurança e os requisitos para a contratação de serviços de processamento de dados, armazenamento e computação em nuvem a serem observados pelas instituições autorizadas a funcionar pelo Banco Central do Brasil.	01/07/2021
Brazil	**Law No. 13,709/18 - LGPD**	Regulamentação local de proteção de dados.	18/09/2020
Portugal	**Data privacy and cybersecurity regulation: Law no. 46/2018**	A Lei n.º 46/2018, de 13 de agosto, estabelece o quadro jurídico para a segurança do ciberespaço, transpondo a Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e dos sistemas de informação em toda a União Europeia.	09/08/2023
Portugal	**Cybersecurity regulation: Decree-Law no. 65/2021**	O Decreto-Lei n.º 65/2021, de 30 de julho, procede à implementação, na ordem jurídica nacional, das obrigações decorrentes do Regulamento (UE) 2019/881 do Parlamento Europeu e do Conselho, de 17 de abril de 2019, que permite a implementação de um quadro nacional de certificação da cibersegurança.	14/08/2018
Portugal	**Loi nationale sur la protection des données personnelles (loi n° 58/2019, du 8 août, qui assure la mise en œuvre du GDPR).**	Assegura a aplicação no direito nacional do Regulamento (UE) 2016/679(RGPD) do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.	09/08/2019
Portugal	**CER - Directive (EU) 2022/2557**	Diretiva relativa à resiliência das entidades críticas	
Portugal	**NIS 1 - Directive (EU) 2016/1148**	Diretiva relativa ao nível comum de cibersegurança na UE (Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho, de 6 de julho de 2016);	
Portugal	**NIS 2 - Directive (EU) 2022/2555**	Diretiva relativa a medidas para um elevado nível comum de cibersegurança (Diretiva (UE) 2022/2555, de 14 de dezembro de 2022, que revoga o SRI 1)	
Portugal	**Instruction no. 21/2019 of the Bank of Portugal**	Regula a comunicação de incidentes de cibersegurança em entidades supervisionadas pelo Banco de Portugal e instituições de crédito significativas	

		sediadas em Portugal supervisionadas pelo Banco Central Europeu (BCE).	
Spain	**Law 36/2015, National Security**	Definir os principais atores da Segurança Nacional, sua organização, coordenação e gestão de crises.	28/09/2015
Spain	**Royal Decree 311/2022 ENS**	Regulamenta o regime de segurança nacional e o uso e aplicação de meios eletrônicos, garante a segurança da informação tratada nesses meios.	03/05/2022
Spain	**Royal Decree-Law 12/2018**	Segurança da informação de redes e sistemas. Estabelecer mecanismos para proteger novamente as redes e informações do Sistema.	30/03/2022
Spain	**Regulation (EU) 2016/679 GDPR**	Regula o tratamento que pessoas e empresas fazem em relação a dados pessoais na Europa.	25/05/2018
Spain	**Organic Law 3/2018 LOPD**	Regula o tratamento que as pessoas e empresas fazem em relação aos dados pessoais na ESPANHA.	09/05/2023
Ireland	**Cross Industry Guidance in respect of Information Technology and Cybersecurity Risks - Central Bank of Ireland**	A orientação articula as expectativas do Banco Central em relação à gestão de risco e governança de TI, outsourcing de TI e cibersegurança, abordando questões-chave como alinhamento de TI e estratégia de negócios, risco de outsourcing, gestão de mudanças, segurança cibernética, resposta a incidentes, recuperação de desastres e continuidade de negócios.	
Ireland	**General Portable Storage Device Recommendations - Data Protection Commission**	Recomendações para o uso de dispositivos de armazenamento portáteis e requisito de notificação de violação	
Italy	**Supervisory provisions for banks Circular No. 285 of December 17, 2013 - Central Bank of Italy**	O Banco de Itália emitiu recentemente a 40.ª atualização da Circular n.º 285/2013 sobre "Provisões de Supervisão para os Bancos", através da qual o Capítulo 4 (O Sistema de Informação) e o Capítulo 5 (Continuidade de Negócios) foram alterados para implementar as "Orientações sobre Gestão de Riscos e Segurança das Tecnologias da Informação (ICT)" emitidas pela EBA em 28 de novembro de 2019, com as quais as regulamentações nacionais já estão amplamente em conformidade.	
Italy	**EBA Guidelines on ICT and security risk management (EBA/GL/2019/04)**	As orientações da EBA estabelecem um quadro harmonizado de medidas de gestão de riscos relacionadas com a utilização das tecnologias da informação e da comunicação (TIC) e as medidas de segurança que os bancos devem ter em	

		vigor. As orientações destinam-se aos prestadores de serviços de pagamento, às instituições de crédito e às empresas de investimento.	
Italy	**Business Continuity (Circular 285)**	A Circular 285 refere-se expressamente à responsabilidade das filiais no que diz respeito à "continuidade dos negócios": para as filiais italianas de intermediários estrangeiros, a coordenação do plano de continuidade de negócios relativo a processos sistemicamente importantes é assegurada pelas próprias sucursais, em estreita ligação com as estruturas que gerem a continuidade das atividades a nível central ou geográfico	
Italy	**Information system**	"Sistema de informação" refere-se apenas aos bancos italianos e filiais de bancos não pertencentes à UE: Estas disposições aplicam-se: - aos bancos italianos e filiais de bancos não pertencentes à UE, com excepção dos sediados nos Estados indicados no anexo A das disposições introdutórias (5); - estes últimos só aplicam estas disposições no que se refere à prestação de serviços de pagamento;	
Korea	**ELECTRONIC FINANCIAL TRANSACTIONS ACT (Act No.17354)**	O objetivo desta Lei é garantir a segurança e a confiabilidade das transações financeiras eletrônicas, esclarecendo suas relações jurídicas e promover conveniências financeiras para as pessoas e contribuir para o desenvolvimento econômico nacional, criando uma base para o desenvolvimento sólido da indústria financeira eletrônica.	10/12/2020
Korea	**ACT ON THE DEVELOPMENT OF CLOUD COMPUTING AND PROTECTION OF ITS USERS (Act No.18738)**	O objetivo desta Lei é contribuir para a melhoria da qualidade de vida e o desenvolvimento da economia nacional, promovendo o desenvolvimento e o uso da computação em nuvem e criando um ambiente para o uso seguro dos serviços de computação em nuvem.	12/01/2023
Korea	**PERSONAL INFORMATION PROTECTION ACT (Act No.19234)**	O objetivo desta Lei é proteger a liberdade e os direitos dos indivíduos e, além disso, realizar a dignidade e o valor dos indivíduos, prescrevendo o processamento e a proteção de informações pessoais.	15/09/2023

07 FRAMEWORK PARA A DEFINIÇÃO DE OBJETIVOS DA SEGURANÇA CIBERNÉTICA

Os objetivos de cibersegurança do Mobilize Financial Services Group são determinados e atualizados considerando:

- a estratégia do Grupo Mobilize Financial Services;
- contexto interno e externo;
- as necessidades e expectativas das partes interessadas na cibersegurança do Mobilize Financial Services Group;
- o estado dos riscos cibernéticos para o Mobilize Financial Services Group.

Estes objetivos são especificados todos os anos no Roteiro para a Cibersegurança.

O Roteiro de Segurança Cibernética contém:

- Um resumo;
- Uma revisão do contexto e das necessidades das partes a atualizar;
- Apresentação do(s) sistema(s) de gestão da cibersegurança;
- Indicadores de conformidade, informações sobre não conformidades pendentes e conclusões da(s) revisão(ões) gerencial(is);
- Apresentação de realizações e ações a serem tomadas para melhoria contínua e correção de não conformidades.

Para cada princípio chave de cibersegurança, o roteiro de cibersegurança apresenta:

- Desafios;
- Pontos fortes;
- Fraquezas;
- Riscos;
- O status do plano de ação definido no roteiro de cibersegurança anterior;
- O plano de ação para o próximo ano para alcançar os objetivos de cibersegurança.

08 REGRAS DE GESTÃO DE EXCEÇÕES

O Diretor de Informações de Segurança do Grupo Mobilize Financial Services deve definir, implantar, verificar e melhorar um processo para gerenciar solicitações de exceções à aplicação da Política de Cibersegurança, a fim de entender as questões de negócios e segurança cibernética, identificar, analisar e avaliar os riscos relacionados a essa exceção e determinar se uma exceção deve ser concedida.

09 HISTORICO E VALIDAÇÕES

	Name	Function	Date and signature
Mobilize Financial Services Group Editor(s) – Banking rules	Kévin VYAS	Gerente de Projetos de Segurança Cibernética	23/01/2024
	Loubna MANSOURI	Consultor externo (Neotrust)	23/01/2024
Mobilize Financial Services Owner(s)	François VOTO	Chefe do departamento de risco, conformidade e segurança	24/01/2024
	Stergios RAPTIS	Diretor de Segurança da Informação (CISO)	24/01/2024
Mobilize Financial Services Group Validators	Umberto MARINI	Diretor de Informática	25/01/2024
	Marc LAGRENE	Diretor de Riscos	25/01/2024
Mobilize Financial Services Group Validators Approvers	Executive Board (ComEx)	Membros ComEx	29/01/2024
Mobilize Financial Services Group Validators Approvers	Supervisory Board (Risk committee)	Risk committee members	02/02/2024

Version History			
Version	**Date of application**	**Purpose of the main changes**	**Editor**
1.0	05/02/2024	Status do MFS ISSP versão 2024 atualizado: Aprovado	Stergios RAPTIS