Unida DTVM

Unida
UNIDA D.T.V.M.

Resumo Detalhado – Política de Segurança Cibernética e de Processamento e Armazenamento de Dados em Nuvem

1. Objetivos

Esta Política estabelece as diretrizes e normas para a segurança cibernética e o uso de serviços em nuvem na **UNIDA DTVM LTDA**, em conformidade com as melhores práticas e exigências regulatórias. Seus principais objetivos são:

- Divulgar os Princípios: Apresentar as diretrizes e a postura estratégica da **UNIDA DTVM LTDA** sobre o tema, visando proteger os dados de clientes, colaboradores e da própria instituição com base nos pilares de confidencialidade, integridade, disponibilidade e finalidade.
- Aumentar a Resiliência: Elevar a resistência da instituição a ataques cibernéticos e incidentes relacionados à Tecnologia da Informação.
- Definir Responsabilidades: Atribuir papéis e responsabilidades claras a todos os colaboradores, prestadores de serviços e fornecedores em relação à segurança dos dados.
- Garantir Conformidade: Assegurar que os requisitos legais e regulatórios sobre segurança cibernética e uso de dados em nuvem sejam conhecidos e cumpridos por todos.
- Promover a Cultura de Segurança: Disseminar uma cultura organizacional de segurança, com o compromisso da alta administração com a melhoria contínua e a prevenção de incidentes.
- Prevenir e Detectar: Declarar os esforços da instituição para prevenir, detectar e reduzir a vulnerabilidade a incidentes cibernéticos.

2. Público-Alvo e Abrangência

Esta política é um documento mandatório para todos os funcionários, colaboradores e prestadores de serviços (pessoas físicas ou jurídicas) da **UNIDA DTVM LTDA**, incluindo:

- Administradores, gestores e membros do Comitê.
- Colaboradores envolvidos em processos que utilizem tecnologia da informação, dados e documentos da instituição.
- Responsáveis pelo desenvolvimento, teste, aquisição e contratação de soluções de tecnologia.
- Responsáveis pela guarda, recuperação e destruição de equipamentos físicos que contenham dados relevantes.
- Prestadores de serviços e fornecedores de produtos de tecnologia, processamento de dados e computação em nuvem.

3. Declaração Institucional

A **UNIDA DTVM LTDA** declara seu firme compromisso com a proteção de toda e qualquer informação sob sua guarda contra acessos ou usos não autorizados. A instituição busca

ativamente conhecer, registrar e minimizar todas as vulnerabilidades cibernéticas a que possa estar exposta.

É inaceitável que, por desconhecimento, omissão ou negligência de seus colaboradores ou parceiros, clientes ou a própria instituição sejam expostos a vulnerabilidades não gerenciadas. Fomentamos uma cultura organizacional que valoriza a segurança cibernética, da informação e de tecnologia , por meio de treinamentos e comunicação clara e acessível.

Reafirmamos nossa disposição em compartilhar informações sobre incidentes relevantes com o Banco Central do Brasil e outras instituições, visando o fortalecimento do ecossistema financeiro.

4. Conformidade e Governança

4.1. Conformidade

Esta política atende aos requisitos de segurança, confidencialidade, integridade e disponibilidade de dados contidos nos seguintes normativos:

- Lei nº 12.527/2011 (Lei de Acesso à Informação).
- Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais - LGPD).
- Resolução BCB nº 85/2021, que dispõe sobre a política de segurança cibernética e a contratação de serviços em nuvem.
- Resolução BCB nº 368/2024, que atualiza o escopo de aplicação de diversas normas para DTVMs e CTVMs.
- Outras resoluções e comunicados aplicáveis do Banco Central do Brasil.

4.2. Governança

- Responsabilidade: O conteúdo desta política é de responsabilidade do Diretor registrado no Unicad do Banco Central do Brasil como responsável pela Política de Segurança Cibernética.
- Gestão: A elaboração, guarda, divulgação e controle de versões são de responsabilidade do Gerente de Compliance.
- Aprovação: A política é aprovada pelo Diretor responsável e pelos Diretores Executivos da instituição.
- Revisão: O documento é reavaliado sempre que houver alterações relevantes na instituição ou em requisitos legais, não possuindo um prazo de validade fixo.
- Divulgação: Um resumo público desta política está disponível no site da **UNIDA DTVM LTDA** (www.unidadtvm.com.br).

5. Diretrizes de Segurança

5.1. Procedimentos e Controles

A **UNIDA DTVM LTDA** possui mecanismos de controle específicos para:

- Segurança de Tecnologia da Informação:
  - Proteção contra softwares maliciosos e verificação periódica de ameaças.
  - Manutenção de cópias de segurança (backups) armazenadas em locais físicos distintos dos originais, com testes regulares de integridade.
  - Controle de acesso e segmentação da rede de computadores.
  - Segurança física do ambiente de TI, com proteção contra incêndio e falhas de energia.
  - Atualização periódica dos sistemas operacionais conforme recomendação dos fornecedores.
- Segurança Cibernética:
  - Adoção de

firewalls e realização periódica de testes e varreduras para detecção de vulnerabilidades.

  - Revisão periódica dos privilégios de acesso dos usuários a sistemas e equipamentos.
  - Cancelamento imediato de acessos em caso de demissões, término de contratos ou suspeita de uso indevido.
  - Armazenamento seguro de senhas por meio de criptografia.
- Segurança da Informação:
  - Estabelecimento de mecanismos de rastreabilidade, como LOGs e trilhas de auditoria, para registrar as ações dos usuários nos dados.
  - Implementação de controles específicos para garantir a segurança de informações pessoais e sensíveis.

5.2. Classificação da Informação

As informações são classificadas com base em dois eixos para determinar o nível de proteção adequado:

- Criticidade (Baixo, Médio, Alto, Crítico): Avalia o impacto da exposição dos dados sobre as partes interessadas (clientes, funcionários, parceiros, etc.).
- Sensibilidade (Baixo, Médio, Alto, Crítico): Avalia o tipo de dado, diferenciando entre dados públicos, anonimizados, pessoais e pessoais sensíveis (conforme a LGPD).

O descarte de informações, seja em meio físico ou digital, segue procedimentos seguros como desmagnetização, limpeza criptográfica (*wiping*) e trituramento físico, com registro formal do processo.

5.3. Gestão de Incidentes Cibernéticos e Resiliência

- **Notificação:** Qualquer funcionário, colaborador ou prestador de serviço que identifique um evento adverso (ex: tentativas de acesso não autorizado, uso indevido de senhas, sistemas desatualizados) deve notificar imediatamente o departamento de Gerenciamento de Riscos.
- **Plano de Resposta:** Os incidentes são registrados e analisados conforme um Plano de Resposta a Incidentes, que define as responsabilidades, os fluxos de comunicação e os procedimentos para mitigar os impactos.
- **Comunicação:** Incidentes de alta criticidade são comunicados à diretoria executiva, que decide sobre a eventual comunicação ao Banco Central do Brasil e aos titulares dos dados.
- **Resiliência:** As estratégias de resiliência estão integradas ao Plano de Continuidade de Negócios (PCN), que prevê a recuperação de operações em cenários de indisponibilidade. Testes periódicos, incluindo simulações de ataques, são conduzidos ao menos anualmente para validar os procedimentos.

5.4. Cultura de Segurança e Treinamento

A instituição mantém um Programa Estruturado de Conscientização em Segurança Cibernética, que inclui:

- **Treinamentos Obrigatórios:** Todos os colaboradores, terceiros e prestadores de serviços devem participar de treinamentos regulares sobre uso seguro de dispositivos, prevenção a golpes de engenharia social, criação de senhas fortes e proteção de dados pessoais.
- **Comunicação Contínua:** São promovidas "pílulas educativas", simulações de *phishing* e comunicados periódicos para reforçar a cultura de segurança no dia a dia.
- **Adesão Formal:** Novos colaboradores são apresentados à política no momento da contratação e devem assinar um termo de compromisso.

5.5. Serviços em Nuvem e Gestão de Fornecedores

- **Avaliação de Relevância:** A contratação de serviços em nuvem é precedida de uma avaliação que classifica o serviço como de Baixa, Média ou Alta relevância, com base na criticidade para o negócio e na sensibilidade dos dados envolvidos.
- **Due Diligence:** Antes de contratar um provedor de média ou alta relevância, a **UNIDA DTVM LTDA** verifica sua capacidade de cumprir a legislação, garantir a confidencialidade e disponibilidade dos dados, e sua aderência a certificações de segurança. A contratação de serviços no exterior segue regras ainda mais estritas.
- **Cláusulas Contratuais:** Todos os contratos com fornecedores relevantes devem conter cláusulas específicas de segurança, exigindo confidencialidade,

notificação imediata em caso de incidentes e o direito de auditoria pela **UNIDA DTVM LTDA**.

5.6. Plano de Ação e Relatório Anual

- Plano de Ação: A área de Tecnologia da Informação elabora e revisita anualmente um plano de ação e de resposta a incidentes, que descreve as rotinas, controles e projetos para implementar as diretrizes desta política.
- Relatório Anual: Até 31 de março de cada ano, é elaborado um relatório com data-base de 31 de dezembro do ano anterior. Este relatório detalha a efetividade das ações, os incidentes relevantes ocorridos, as medidas corretivas e os resultados dos testes de continuidade, sendo submetido ao comitê diretivo.

6. Responsabilidade e Sanções

O cumprimento desta política é mandatório. A negligência, culpa ou dolo no descumprimento dos requerimentos aqui estabelecidos sujeitará os envolvidos às seguintes sanções:

- Para a **UNIDA DTVM LTDA** e seus Administradores (pelo Banco Central do Brasil):
  - Admoestação pública.
  - Multas.
  - Proibição de realizar determinadas atividades ou inabilitação para cargos de administração.
  - Cassação da autorização para funcionamento.
- Para Funcionários e Colaboradores (internamente):
  - Advertência (oficiosa ou formal).
  - Suspensão temporária.
  - Demissão ou rescisão de contrato.

UNIDA DTVM

www.unidadtvm.com.br

Compliance

[11] 3506-5500

Alameda Rio Negro, 500 - Alphaville

compliance-ci@unidadtvm.com.br