Política de Segurança da Informação Externa

Sistema de Gestão

Sumário

Controle de versão

Data	Versão	Autor	Escopo
2020-10-02	2.0	Clodoaldo Bragato	Versão Inicial

1. Propósitos e princípios da política de segurança da informação externa

Implementar as melhores práticas de segurança da informação, tendo por finalidade atribuir responsabilidades, definir direitos, deveres, expectativas de acesso e uso, penalidades e promover uma cultura de proteção aos dados e à informação da **MIX REALITY**, de clientes, fornecedores e de parceiros.

Estabelecer as diretrizes para criação, transmissão, processamento, utilização, armazenamento, recuperação e descarte de informações de modo a preservar as informações quanto aos seguintes princípios:

- **Integridade:** garantia de que a informação seja mantida em seu estado original, exata e completa;
- **Confidencialidade:** garantia de que o acesso à informação esteja disponível somente para pessoas, entidades ou processos autorizados;
- **Disponibilidade:** garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

A **Mix Reality** considera em suas políticas de segurança da informação o processo contínuo no qual os riscos são identificados, analisados, avaliados, tratados e reduzidos a um nível aceitável.

2. Referência

- NBR ISO IEC 27001: 2013
- NBR ISO IEC 27002: 2013

3. Responsabilidades

3.1. Colaborador externo

3.1.1. É da responsabilidade de cada colaborador externo, o prejuízo ou dano que vier a sofrer ou causar à **MIX REALITY** ou a terceiros em decorrência da não obediência às diretrizes desta política.

3.1.2. Notificar os incidentes, fragilidades ou ainda, suspeitas de fragilidades de segurança da informação observadas na **MIX REALITY**.

3.2. Comitê de Segurança da Informação da MIX REALITY

3.2.1. É responsável pela análise das infrações cometidas pelos colaboradores externos frente a esta política, com consequência de incidente, devendo examinar a gravidade e riscos sob o enfoque técnico e legal de cada infração cometida, resultando na recomendação de processo disciplinar para apuração dos fatos e aplicação das ações disciplinares cabíveis, para eventual e futuro encaminhamento às autoridades policiais ou judiciais, quando necessário.

3.2.2. Este Comitê poderá ser contatado a qualquer momento pelos colaboradores externos para esclarecer dúvidas, obter orientações, expressar opiniões, reportar situações de violação a esta política ou outros eventos de segurança da informação, por meio da conta corporativa de *e-mail* csi@mixreality.com.

4. POLÍTICA DE CONTROLE DE ACESSO

4.1. É de responsabilidade do colaborador externo, quaisquer acessos realizados com o identificador/login e o mesmo deve ser único, pessoal e intransferível.

4.2. O colaborador externo, vinculado a tais dispositivos identificadores, é responsável pelo seu uso correto perante a instituição e a legislação (cível e criminal).

4.3. Deverá constar para os contratados e contratantes da **MIX REALITY** o Acordo de Responsabilidade e Confidencialidade da Informação, ou equivalente, como condição imprescindível para execução do contrato.

4.4. O acesso à informação e às funções dos sistemas de aplicação devem ser restringidos por meio de controle dos direitos de acesso dos colaboradores de forma a limitar quais dados ou funções dos sistemas de aplicação poderão ser acessados por determinado colaborador e qual o nível de permissão.

4.5. Todos os acessos devem ser imediatamente bloqueados quando se tornarem desnecessários.

5. POLÍTICA DE CLASSIFICAÇÃO E TRATAMENTO DA INFORMAÇÃO

5.1. Os contratantes deverão ter controles de segurança aplicados aos seus ativos tecnológicos que armazena, processa e manuseia a informação da **Mix Reality** e de seus contratados, com o tratamento apropriado à sensibilidade e criticidade operacional, conforme classificada pela **Mix Reality**.

5.2. Os contratados deverão ter controles de segurança aplicados aos seus ativos tecnológicos que armazena, processa e manuseia a informação da **Mix Reality** e de seus contratantes, com o tratamento apropriado à sensibilidade e criticidade operacional, conforme classificada pela **Mix Reality**.

5.3. A informação da **Mix Reality,** de seus clientes e de seus fornecedores, seja ela eletrônica, física ou verbal deve ser apropriadamente protegida, independente dos meios pelos quais é compartilhada.

5.4. Classificação da informação quanto ao sigilo:

Classificação	PÚBLICA	CORPORATIVA	CONFIDENCIAL	SECRETA
Impacto quanto à perda de Confidencialidade	Inexistente	Baixo	Médio	Alto
Definição	Pode ser divulgada a qualquer pessoa sem que haja implicações à **Mix Reality**. O conhecimento desta informação pelo público não expõe a organização a prejuízo financeiro, constrangimento, tampouco compromete a	São restritas ao âmbito da **Mix Reality**. Porém, se ocorrer divulgação externa das informações ou comprometimento, as consequências não são críticas.	Informações que a **Mix Reality** ou seus contratados têm a obrigação legal, regulamentar ou social de proteger. Divulgação não autorizada teria um impacto adverso à organização. Dado Pessoal é confidencial. Dado de Cliente é confidencial.	Informações estratégicas e financeiras, cuja divulgação não autorizada pode resultar em danos graves, proporcionar vantagem significativa para um concorrente, ou incorrer em consequências financeiras graves para a organização,

	segurança dos ativos.			parceiros e contratantes.

6. POLÍTICA PARA USO DOS ATIVOS

6.1. O colaborador externo deve zelar pelo bom uso dos recursos de informática a ele disponibilizados não removendo, alterando ou acrescentando, qualquer tipo de componente interno de hardware ou software.

6.2. O uso das mídias removíveis deve ser evitado. É imprescindível o uso de criptografia ao armazenar em mídia removível informação com mais alto grau de sensibilidade.

6.3. O colaborador externo não deve consumir alimentos e bebidas muito próximo aos recursos tecnológicos e aos documentos físicos que contenham informações da MIX REALITY, de seus clientes ou de seus fornecedores podendo ser responsabilizado por danos causados em decorrência deste ato.

7. POLÍTICA PARA TRANSFERÊNCIA DE INFORMAÇÕES.

7.1. Os requisitos para confidencialidade da informação estão descritos no Acordo de Responsabilidade e Confidencialidade da Informação ou equivalente.

7.2. Os contratados da MIX REALITY devem ser extremamente cautelosos na utilização de quaisquer meios de comunicação, ficando proibida qualquer troca de informações sem autorização, justificativa e criptografia com outros que contenham qualquer referência a:

7.2.1. Documentação dos sistemas (código fonte, diagramas, documentação de tabelas, especificações funcionais, especificações técnicas, wireframes, e qualquer outro documento que componha o projeto de software);

7.2.2. Diagramas, propostas, *checklists* operacionais, projetos, *papers* técnicos ou da empresa;

7.2.3. Decisões sobre aquisições, fusões, incorporações;

7.2.4. Patentes, pesquisas, desenvolvimento de *software* e de soluções.

8. POLÍTICA PARA TRABALHO REMOTO

8.1. A concessão do acesso remoto via VPN à contratada ou contratante será de exclusivo critério da MIX REALITY e mediante solicitação por meio de processo formal, que optará por qual rede o colaborador externo terá permissão de acesso. A referida concessão será feita de forma individual, sendo os colaboradores externos responsáveis por seus acessos via VPN, bem como, por qualquer atividade irregular exercida por outra pessoa de posse de seu acesso remoto. Com isso, os colaboradores externos deverão adotar medidas de cautela, para que terceiros não tenham acesso, sem autorização, à sua conexão de VPN.

8.2. O colaborador externo deve retirar imediatamente da impressora os documentos que tenha solicitado a impressão caso contenham informações sensíveis.

9. POLÍTICA PARA PROTEÇÃO DE INFORMAÇÃO PESSOAL

9.1. A MIX REALITY deve garantir por meio de contrato que o propósito do tratamento dos dados pessoais de colaboradores MIX REALITY e de seus contratantes não seja ilícito ou abusivo por parte de seus contratados.

9.2. A MIX REALITY deve garantir por meio de contrato que o propósito do tratamento dos dados pessoais de colaboradores MIX REALITY e de seus contratados não seja ilícito ou abusivo por parte de seus contratantes.

9.3. Devem ser observadas pelos contratantes e contratados, as legislações e regulamentações vigentes que versam sobre:

9.3.1. Os direitos fundamentais à privacidade e à intimidade (Constituição Federal);

9.3.2. O *habeas data*, ação que permite ao indivíduo o conhecimento e a retificação de dados pessoais constantes de registros públicos ou banco de dados de entidades governamentais ou de caráter público;

9.3.3. A lei que dispõe sobre a apresentação e uso de documentos de identificação pessoal (lei nº 5.553);

9.3.4. Disposições específicas do Direito do Consumidor;

9.3.5. Legislação bancária e fiscal;

9.3.6. Lei 10.406/2002 – Código Civil Brasileiro;

9.3.7. LGPD – Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709, de 14 de agosto de 2018 - Alterada pela Lei nº 13853, de 2019).

10. Tratamento das Exceções

10.1. As exceções a esta política devem ser explicitadas, autorizadas e formalizadas em procedimentos, em Acordo de Responsabilidade e Confidencialidade da Informação Externo ou equivalente.

10.2. Devem ser definidos e implementados controles de segurança para minimizar os riscos inerentes às exceções a esta política.

11. Processo Disciplinar

11.1. O colaborador externo tem por obrigação cumprir esta política. Desta forma, o não cumprimento será considerado uma infração.

11.2. Por meio do Comitê de Segurança da Informação, a MIX REALITY exercerá seu poder para determinar sanções aos infratores. A infração será classificada em 3 níveis:

11.2.1. Incidente leve: quando há perda de um dos critérios CIDAL de informação classificada como corporativa;

11.2.2. Incidente médio: quando há perda de um dos critérios CIDAL de informação classificada como confidencial;

11.2.3. Incidente grave: quando há perda de um dos critérios CIDAL de informação classificada com mais alto grau de sensibilidade. Ou quando denigra a imagem da **MIX REALITY**. São considerados ainda incidentes graves, as tentativas deliberadas de acesso não autorizado a dados secretos, bem como atividades ilícitas vinculadas a ações de “corrupção”, “fraude”, “conluio”, “má-fé contratual”, “terrorismo”, “pedofilia” e “comercialização de drogas”.

11.3. Diante da constatação de um incidente já devidamente classificado, no caso de colaboradores terceirizados, será solicitado à empresa prestadora da respectiva mão de obra, o afastamento temporário ou definitivo do funcionário, conforme a falta cometida podendo em último caso, a MIX REALITY solicitar a rescisão do contrato de prestação de serviço.

11.4. Não existe uma ordem para a aplicação das sanções, sendo assim, uma infração pode ter punição máxima sem que tenha cometido qualquer outra infração anterior.

11.5. A aplicação destas sanções não isenta o colaborador externo de sofrer outras penalidades previstas em contratos, ou mesmo de sofrer processos penais por crimes de condescendência criminosa, de violação de sigilo funcional entre outros, estabelecidos no código penal.

11.6. Diante da omissão ou inércia daquele que tiver ciência ou que desconfie da ocorrência de incidente relacionado à segurança da informação, este poderá ser responsabilizado na medida de sua omissão.