POLÍTICA DE SEGURANÇA CIBERNÉTICA MELVER

1. DEFINIÇÕES

Acionistas Fundadores: Raony Bourscheidt Rossetti, Jaqueline Bourscheidt Rossetti e Nasser Bassyouny Said.

Acionista Controlador: O acionista ou grupo de acionistas, vinculado(s) por acordo ou sob controle comum, que exerça(m) o poder de controle, direto ou indireto, sobre sociedade, nos termos da Lei nº 6.404/76.

Administradores: São os membros da Diretoria e do Conselho de Administração da Companhia, titulares e suplentes.

Colaboradores MELVER: Acionistas, funcionários, empregados, estagiários, prestadores de serviços, empresas contratadas e seus respectivos funcionários, criadores, cocriadores, desenvolvedores, programadores, divulgadores, professores, conteudistas, freelancers, consultores, produtores de conteúdo, pessoas físicas ou jurídicas relacionados à MELVER.

Companhia: MELVER S.A.

Plataforma MELVER: É a plataforma de ensino e negócios desenvolvida e patenteada pela MELVER.

Sistemas de Comunicação: Aplicativos de comunicação eletrônicos, videoconferências, mensagens, voz, e-mails, telefonia, sistemas de *Customer Relationship Management*, correspondências, Serviço de Atendimento ao Consumidor, redes, aplicativos e mídias sociais e canais próprios, de uso particular ou comercial da MELVER e dos Colaboradores MELVER.

Terceiros Relacionados à MELVER: Consumidores, clientes, parceiros, fornecedores, prestadores de serviços, alunos, leads, interessados e usuários da MELVER.

2. OBJETIVO

A Política de Segurança Cibernética da MELVER visa garantir a proteção, a manutenção da privacidade, integridade, disponibilidade e confidencialidade das informações de sua propriedade e/ou sob sua guarda, além de prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados com o ambiente cibernético, definindo as regras que representam, em nível estratégico, os princípios fundamentais incorporados pela MELVER para o alcance dos objetivos de segurança da informação.

A Política de Segurança Cibernética da MELVER demonstra o compromisso da MELVER e seus acionistas em zelar e tratar as informações de seus clientes, de forma a proporcionar plena satisfação quanto à segurança e privacidade de suas informações. Demonstramos também o compromisso da MELVER com os aspectos regulatórios e estratégicos da Companhia, estando assim, em conformidade com as principais regulamentações vigentes.

3. VIGÊNCIA

A Política de Segurança Cibernética da MELVER entrará em vigor na data de sua divulgação na Plataforma MELVER, e eventualmente compartilhado nos Sistemas de Comunicação, e poderá ser revisada anualmente ou, quando necessário, caso ocorra alguma alteração nas normas da MELVER, alteração de diretrizes de segurança da informação, objetivos de negócio ou se requerido por órgãos reguladores.

4. PRINCÍPIO DE SEGURANÇA DA INFORMAÇÃO

A MELVER compreende que os ativos de informação são um dos bens mais importantes no mercado, portanto, tratá-los com responsabilidade é compromisso fundamental a ser observado pela Companhia. Dessa forma, a MELVER baliza suas atividades norteada pelos princípios de segurança da informação, cujo objetivos constituem a preservação da propriedade da informação, notadamente sua confidencialidade, integridade e disponibilidade, permitindo o uso e

compartilhamento de forma controlada, bem como o monitoramento e tratamento de incidentes provenientes de ataques cibernéticos.

Confidencialidade: garantir que as informações tratadas sejam de conhecimento exclusivo de pessoas especificamente autorizadas;

Integridade: garantir que as informações sejam mantidas íntegras, sem modificações indevidas – acidentais ou propositais;

Disponibilidade: garantir que as informações estejam disponíveis a todas as pessoas autorizadas a tratá-las.

5. INFORMAÇÕES CONFIDENCIAIS

O acesso às informações confidenciais, incluindo dados pessoais, coletadas e armazenadas pela MELVER é restrito aos profissionais autorizados ao uso direto dessas informações, e necessário à prestação de seus serviços, sendo limitado o uso para outras tarefas. A MELVER preza pela privacidade das informações no âmbito da Lei Geral de Proteção de Dados ("LGPD") e da Política de Privacidade de Dados.

A MELVER poderá revelar as informações confidenciais nas seguintes hipóteses:

i. Sempre que estiver obrigada a revelá-las, seja em virtude de dispositivo legal, ato de autoridade competente, ordem ou mandado judicial;
ii. Aos órgãos de proteção e defesa de crédito e prestadores de serviços autorizados pela MELVER a defender seus direitos e créditos.

6. ESTRUTURA DE GERENCIAMENTO DE SEGURANÇA CIBERNÉTICA

O gerenciamento dos controles de segurança objetiva assegurar que os procedimentos operacionais sejam desenvolvidos, implantados e mantidos ou modificados de acordo com os objetivos estabelecidos nesta Política de Segurança Cibernética da MELVER.

6.1. GESTÃO DE ACESSOS ÀS INFORMAÇÕES

Os acessos às informações são controlados, monitorados, restringidos à menor permissão e privilégios possíveis, revistos periodicamente, e cancelados tempestivamente ao término do contrato de trabalho ou do prestador de serviço dos Colaboradores MELVER.

Os equipamentos e instalações de processamento de informação crítica ou sensível são mantidos em áreas seguras, com níveis de controle de acesso apropriados, somente tendo o acesso pessoas autorizadas, incluindo proteção contra ameaças físicas e ambientais.

6.2. PROTEÇÃO DO AMBIENTE DO GRUPO

São constituídos controles e responsabilidades pela gestão e operação dos recursos de processamento das informações, visando garantir a segurança na infraestrutura tecnológica da MELVER por meio de um gerenciamento efetivo no monitoramento, tratamento e na resposta aos incidentes, com o intuito de minimizar o risco de falhas e a administração segura de redes de comunicações.

6.2.1. AUTENTICAÇÃO

O acesso às informações e aos ambientes tecnológicos da MELVER deve ser permitido apenas às pessoas autorizadas pela MELVER, levando em consideração o princípio do menor privilégio, a segregação de funções conflitantes e a classificação da informação.

O controle de acesso aos sistemas deve ser formalizado e contemplar, no mínimo, os seguintes controles:

i. A utilização de identificadores (credencial de acesso) individualizados, monitorado e passíveis de bloqueios e restrições (automatizados e manuais);
ii. A remoção de autorizações dadas a Colaboradores MELVER afastados ou desligados da MELVER, ou ainda que tenham mudado de função; e
iii. A revisão periódica das autorizações concedidas.

6.2.2. GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

O comportamento de possíveis ataques é identificado por meio de controles de detecção implementados no ambiente, como filtro de conteúdo, ferramenta de detecção de comportamentos maliciosos, Antivírus, Antispam, entre outros. Os incidentes identificados devem seguir o processo de resposta a incidentes.

6.2.3. PREVENÇÃO A VAZAMENTO DE INFORMAÇÕES

Utilização de controle para prevenção de perda de dados, responsável por garantir que dados confidenciais não sejam perdidos, roubados, mal utilizados ou vazados na web por usuários não autorizados.

6.2.4. TESTES DE INTRUSÃO

Testes de Intrusão interno e externo nas camadas de rede e aplicação devem ser realizados no mínimo anualmente.

6.2.5. VARREDURA DE VULNERABILIDADES

As varreduras das redes internas e externas devem ser executadas periodicamente. As vulnerabilidades identificadas devem ser tratadas e priorizadas de acordo com seu nível de criticidade.

6.2.6. CONTROLE CONTRA SOFTWARE MALICIOSO

Todos os ativos (computadores, servidores etc.) que estejam conectados à rede corporativa ou façam uso de informações da MELVER, devem, sempre que compatível, ser protegidos com uma solução anti-malware determinada pela MELVER.

6.2.7. CRIPTOGRAFIA

Toda solução de criptografia utilizada da MELVER deve seguir as regras de Segurança da Informação e os padrões de segurança dos Órgãos Reguladores.

6.2.8. DESENVOLVIMENTO SEGURO

A MELVER mantém um conjunto de princípios para desenvolver sistemas de forma segura, garantindo que a segurança cibernética seja projetada e implementada no ciclo de vida de desenvolvimento de sistemas.

6.2.9. CÓPIAS DE SEGURANÇA (BACKUP)

O processo de execução de backups é realizado, periodicamente, nos ativos de informação da MELVER, de forma a evitar ou minimizar a perda de dados diante da ocorrência de incidentes.

6.3. CONTINUIDADE DOS NEGÓCIOS

O processo de continuidade de negócios é implementado com o intuito de reduzir os impactos e perdas de ativos da informação após um incidente crítico a um nível aceitável, por meio do mapeamento de processos críticos, análise de impacto nos negócios e testes periódicos de recuperação de desastres. Incluem-se nesse processo, a continuidade de negócios relativos aos serviços contratados na nuvem e os testes previstos para os cenários de ataques cibernéticos.

6.4. PROCESSAMENTO, ARMAZENAMENTO DE DADOS E COMPUTAÇÃO EM NUVEM

Para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem, a MELVER assegura-se de um procedimento efetivo para a aderência às regras previstas na regulamentação em vigor, analisando a idoneidade e competência das empresas prestadoras de serviços deste segmento.

7. PRINCIPAIS RECOMENDAÇÕES DE SEGURANÇA AOS COLABORADORES MELVER E TERCEIROS RELACIONADOS À MELVER

7.1. AUTENTICAÇÃO E SENHA

Todos os Colaboradores MELVER e Terceiros Relacionados à MELVER que, de alguma maneira, obtiverem acesso às áreas restritas da Plataforma MELVER ou intranet da MELVER, são responsáveis pelos atos executados com seu identificador pessoal (login), que é único e acompanhado de senha exclusiva para identificação/autenticação individual no acesso à informação e aos recursos de tecnologia.

A MELVER recomenda que os Terceiros Relacionados à MELVER:

i. Mantenham a confidencialidade, memorizem e não registrem a senha em lugar algum. Ou seja, não contar a ninguém e não anotar em papel;
ii. Alterem a senha sempre que existir qualquer suspeita do comprometimento dela;
iii. Elaborarem senhas de qualidade, de modo que sejam complexas e de difícil adivinhação;
iv. Impeçam o uso do seu equipamento por outras pessoas, enquanto este estiverem conectados/ "logados" com a suas identificações;
v. Bloqueiem sempre o equipamento ao se ausentar.
vi. Sempre que possível, habilitem um segundo fator de autenticação (p.ex.: SMS, Token etc.).

7.2. ANTIVÍRUS

A MELVER recomenda que os Colaboradores MELVER e Terceiros Relacionados à MELVER mantenham uma solução de antivírus atualizada e instalada nos computadores utilizados para acesso aos serviços oferecidos pela MELVER, em especial à Plataforma MELVER. Além disso, a MELVER orienta que os Colaboradores MELVER e Terceiros Relacionados à MELVER possuam o sistema operacional atualizado com as últimas atualizações realizadas.

7.3. ENGENHARIA SOCIAL

A engenharia social, no contexto de segurança da informação, refere-se à técnica pela qual uma pessoa procura persuadir outra, muitas vezes abusando da ingenuidade ou confiança do usuário, objetivando ludibriar, aplicar golpes ou obter informações sigilosas.

7.4. PHISHING

Técnica utilizada por cibercriminosos para enganar usuários, através de envio de e-mails maliciosos, a fim de obter informações pessoais como senhas, cartão de crédito, CPF, número de contas bancárias, entre outros. As abordagens dos e-mails de phishing podem ocorrer das seguintes maneiras:

i. Quando procuram atrair as atenções dos usuários, seja pela possibilidade de obter alguma vantagem financeira, seja por curiosidade ou seja por caridade;
ii. Quando tentam se passar pela comunicação oficial de instituições conhecidas como: Bancos, Lojas de comércio eletrônico, entre outros sites populares;
iii. Quando tentam induzir os usuários a preencher formulários com os seus dados pessoais e/ou financeiros, ou até mesmo a instalação de softwares maliciosos que possuem o objetivo de coletar informações sensíveis dos usuários;

7.5. SPAM

São e-mails não solicitados, os quais geralmente são enviados para muitas pessoas, possuindo tipicamente conteúdo com fins publicitários. Além disso, os Spams estão diretamente associados a ataques de segurança, sendo eles um dos principais responsáveis pela propagação de códigos maliciosos, venda ilegal de produtos e disseminação de golpes.

7.6. FALSO CONTATO TELEFÔNICO

São técnicas utilizadas pelos fraudadores para conseguir informações como dados pessoais, senhas, token, código de identificação do aparelho celular (IMEI) ou qualquer outro tipo de informação para a prática da fraude.

7.7. COMUNICAÇÃO

Quaisquer indícios de irregularidades no cumprimento das determinações desta Política de Segurança Cibernética da MELVER serão alvo de investigação interna e devem ser comunicadas imediatamente aos nossos canais de atendimento.

Última atualização: 15/01/2024.