

Política de Segurança Cibernética

FOLHA DE CONTROLE

Informações Gerais

Título	Política de Segurança Cibernética
Número da Versão	V2
Status	Revisão
Área Proprietária da Política	Segurança da Informação
Escopo do Negócio	NA
Escopo da Geografia	Brasil
Documentos, Procedimentos e Outros Relacionados	Lei nº 13.709 de 2018 – LGPD
Dispensa da Política	NA
Palavras-chave para Procura Rápida	Segurança Cibernética, Incidentes, Invasão, Controles, Rastreabilidade, Cultura, Disseminação

Histórico de Versões

Versão	Motivo da Alteração	Data	Autor	Departamento
1	Versão Inicial Revisão	31/03/2021	Herbert Costa	Tecnologia de Informação

Aprovado por:	Roberto Girelli Mol Diretor	Fábio Girelli Mol Diretor	Suely Girelli Mol Sócia
Data: 15/04/2021			

SUMÁRIO

1.	OBJETIVO	3
2.	VIGÊNCIA	3
3.	PRINCÍPIO DE SEGURANÇA DA INFORMAÇÃO	3
4.	INFORMAÇÕES CONFIDENCIAIS	4
5.	ESTRUTURA DE GERENCIAMENTO DE SEGURANÇA CIBERNÉTICA	4
5.1	GESTÃO DE ACESSOS ÀS INFORMAÇÕES	4
5.2	PROTEÇÃO DO AMBIENTE DA EMPRESA	5
5.2.1	Autenticação	5
5.2.2	Gestão de Incidentes de Segurança da Informação	5
5.2.3	Prevenção a Vazamento de Informações	5
5.2.4	Testes de Intrusão	6
5.2.5	Varredura de Vulnerabilidades	6
5.2.6	Controle Contra Software Malicioso	6
5.2.7	Criptografia	6
5.2.8	Rastreabilidade	6
5.2.9	Segmentação de Rede	6
5.2.10	Desenvolvimento Seguro	7
5.2.11	Cópias de Segurança (Backup)	7
5.3	CONTINUIDADE DOS NEGÓCIOS	7
6.	PRINCIPAIS RECOMENDAÇÕES DE SEGURANÇA AOS CLIENTES e USUÁRIOS	7
6.1	AUTENTICAÇÃO E SENHA	7
6.2	ANTIVÍRUS	8
6.3	ENGENHARIA SOCIAL	8
6.3.1	<i>PHISHING</i>	8
6.3.2	<i>SPAM</i>	9
6.3.3	FALSO CONTATO TELEFÔNICO	9
7.	COMUNICAÇÃO	9
8.	DEFINIÇÕES	9

1. OBJETIVO

A Política de Segurança Cibernética (“Política”) da Motomol Gv LTDA (“empresa”) 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 empresa para o alcance dos objetivos de segurança da informação.

Essa Política demonstra o compromisso da empresa e de sua Alta Administração 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 nosso compromisso com os aspectos regulatórios e estratégicos da empresa, estando assim, em conformidade com as principais regulamentações vigentes.

2. VIGÊNCIA

Esta Política pode ser revisada anualmente ou, quando necessário, caso haja alguma mudança nas normas da empresa, alteração de diretrizes de segurança da informação, objetivos de negócio ou se requerido pelo regulador local.

3. PRINCÍPIO DE SEGURANÇA DA INFORMAÇÃO

Consideramos que os ativos de informação são os bens mais importantes no mercado financeiro, portanto, tratá-los com responsabilidade é o nosso compromisso. Dessa forma, estamos fundamentados nos 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 trata-las.

4. INFORMAÇÕES CONFIDENCIAIS

O acesso às informações confidenciais, incluindo dados pessoais, coletadas e armazenadas pela empresa é restrito aos profissionais autorizados ao uso direto dessas informações, e necessário à prestação de seus serviços, sendo limitado o uso para outras tarefas, devendo respeitar, ainda, o disposto na Norma de Classificação da Informação.

A empresa poderá revelar as informações confidenciais nas seguintes hipóteses:

- Sempre que estiver obrigado a revelá-las, seja em virtude de dispositivo legal, ato de autoridade competente, ordem ou mandado judicial;
- Aos órgãos de proteção e defesa de crédito e prestadores de serviços autorizados pela empresa a defender seus direitos e créditos;
- Para instituições financeiras, empresas de consórcio e a montadora Honda, quando solicitado algum de seus serviços, desde que dentro dos parâmetros legais estabelecidos para tanto, podendo, nesta hipótese, o usuário, a qualquer tempo, cancelar sua autorização.

5. 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.

5.1 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 do colaborador ou do prestador de serviço.

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

Os colaboradores e terceiros da Empresa são treinados, periodicamente, sobre os conceitos de segurança da informação, através de um programa efetivo de conscientização e disseminação da cultura de segurança cibernética.

5.2 PROTEÇÃO DO AMBIENTE DA EMPRESA

São constituídos controles e responsabilidades pela gestão e operação dos recursos de processamento das informações, visando garantir a segurança na infraestrutura tecnológica da empresa 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 da rede de comunicação.

5.2.1 Autenticação

O acesso às informações e aos ambientes tecnológicos da empresa deve ser permitido apenas às pessoas autorizadas pelo Proprietário da Informação, 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:

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

5.2.2 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.

5.2.3 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.

5.2.4 Testes de Intrusão

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

5.2.5 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.

5.2.6 Controle Contra Software Malicioso

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

5.2.7 Criptografia

Toda solução de criptografia utilizada na empresa deve seguir as regras de Segurança da Informação e os padrões de segurança dos Órgãos reguladores.

5.2.8 Rastreabilidade

Trilhas de auditoria automatizadas devem ser implantadas para todos os componentes de sistema para reconstruir os seguintes eventos:

- Autenticação de usuários (tentativas válidas e inválidas);
- Acesso a informações;
- Ações executadas pelos usuários, incluindo criação ou remoção de objetos do sistema.

5.2.9 Segmentação de Rede

- Computadores conectados à rede corporativa não devem ser acessíveis diretamente pela Internet;
- Não é permitida a conexão direta de rede de terceiros utilizando-se protocolos de controle remoto aos servidores conectados diretamente na rede corporativa;

- Para solicitação de criação, alteração e exclusão de regras nos firewalls e ativos de rede, o requisitante deve encaminhar pedido à diretoria da empresa, que fará, junto com a área técnica de TI, a análise e aprovação.

5.2.10 Desenvolvimento Seguro

A empresa, quando necessário o desenvolvimento próprio, 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.

5.2.11 Cópias de Segurança (Backup)

O processo de execução de backups (específicos e também das máquinas virtuais) é realizado, periodicamente, nos ativos de informação da empresa, de forma a evitar ou minimizar a perda de dados diante da ocorrência de incidentes.

5.3 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 internos e também os contratados na nuvem e os testes previstos para os cenários de ataques cibernéticos.

6. PRINCIPAIS RECOMENDAÇÕES DE SEGURANÇA AOS CLIENTES e USUÁRIOS

6.1 AUTENTICAÇÃO E SENHA

O cliente e o usuário são responsáveis pelos atos executados com seu identificador (*login* / sigla), que é único e acompanhado de senha exclusiva para identificação/autenticação individual no acesso à informação e aos recursos de tecnologia.

Recomendamos que:

- Mantenham a confidencialidade, memorizem e não registrem a senha em lugar algum. Ou seja, não contar a ninguém e não anotar em papel;
- Alterarem a senha sempre que existir qualquer suspeita do comprometimento dela;

- Elaborarem senhas de qualidade, de modo que sejam complexas e de difícil adivinhação;
- Impedir o uso de seus equipamentos por outras pessoas, enquanto estes estiverem conectados/ "logados" com suas identificações;
- Bloquear sempre o equipamento ao se ausentarem.
- Sempre que possível, habilitar um segundo fator de autenticação (Por exemplo: SMS, Token e etc.).

6.2 ANTIVÍRUS

Recomenda-se que o cliente, no acesso virtual aos recursos da empresa, mantenha uma solução de antivírus atualizada e instalada no computador utilizado para este acesso. Além disso, possuir o sistema operacional atualizado com as últimas atualizações realizadas

6.3 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.

6.3.1 PHISHING

Técnica utilizada por cibercriminosos para enganar os usuários, através de envio de *e-mails* maliciosos, afim 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:

- Quando procuram atrair as atenções dos usuários, seja pela possibilidade de obter alguma vantagem financeira, seja por curiosidade ou seja por caridade;
- Quando tentam se passar pela comunicação oficial de instituições conhecidas como: Bancos, Lojas de comércio eletrônico, entre outros sites populares;
- 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;

6.3.2 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.

6.3.3 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. COMUNICAÇÃO

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

8. DEFINIÇÕES

Empresa: MOTOMOL GV LTDA.