maps registradora

POLÍTICA DE SEGURANÇA CIBERNÉTICA

VERSÃO 1.1

MARÇO 2024

MAPS Registradora
Política de Segurança Cibernética
Histórico de Revisões

Versão	Data	Histórico
1.0	Setembro 2023	Elaboração do Documento.
1.1	Março 2024	Alterações no assunto "BYOD (*Bring Your Own Device*)"

ÍNDICE

1. Objetivo

O objetivo desta política de cibersegurança é estabelecer diretrizes, princípios e compromissos que visam proteger os ativos digitais, dados sensíveis e sistemas da MAPS Services ("MAPS") contra ameaças cibernéticas, além de definir estratégias e práticas que a empresa deve seguir para garantir a resiliência cibernética.

2. Abrangência

Esta Política é aplicável a todos os colaboradores, gestores e membros da alta administração da MAPS, bem como a terceiros e fornecedores, sempre respeitando os limites determinados nesta Política. A observância desta Política é obrigatória e reflete na proteção e resiliência cibernética da empresa.

3. Diretrizes

Proteção contra códigos maliciosos

Sendo uma empresa que tem a utilização da tecnologia digital como princípio fundamental de funcionamento, a MAPS se preocupa com qualquer código malicioso que crie vulnerabilidades em seus sistemas, violações de segurança, roubo de dados e informações, além de outros danos possíveis que possam impactar seus sistemas de arquivos e computadores.

Para isso, a MAPS implementa, em seu escopo institucional, controles tecnológicos para a proteção de seus equipamentos de processamento de

informação, que executem algum tipo de software, para a prevenção, detecção, correção e erradicação de códigos executáveis maliciosos.

Análise de Vulnerabilidade Técnica Cibernética

Em um cenário cada vez mais complexo e dinâmico, no qual ameaças cibernéticas evoluem constantemente, é crucial adotar uma abordagem proativa para mitigar riscos. Nesse contexto, a análise de vulnerabilidade técnica emerge como um componente essencial de nossa política de segurança da informação, visando identificar e remediar potenciais fraquezas em nossa infraestrutura de tecnologia.

Sendo assim, a MAPS periodicamente deve identificar os riscos internos e externos, bem como os ativos de hardware e software que precisam de proteção, por meio de procedimentos internos, como testes de intrusão (Pentest), e relatórios de antivírus, por exemplo. Esses procedimentos são conduzidos pela equipe de Operações de TI, com o fim de dar visibilidade à metodologia utilizada para avaliar e gerir as vulnerabilidades da MAPS.

O Grupo de Segurança da Informação deve discutir as opções de tratamento a serem adotadas, considerando a seleção de controles para manter os riscos dentro de limites aceitáveis pela MAPS, levando em conta os possíveis impactos financeiros, operacionais e reputacionais, em caso de um evento de segurança, assim como a probabilidade do evento acontecer.

Serviços em Nuvem

Como parte de compromisso contínuo com a segurança cibernética, esta política estabelece as diretrizes para a utilização segura de serviços em nuvem por parte dos colaboradores da MAPS.

A MAPS utiliza internamente serviços em Cloud de seus parceiros e fornecedores, para o uso de seus colaboradores.

Fica estabelecido nesta política que os serviços para processamentos de dados e ou armazenamento em nuvem, sejam eles software como serviço (SaaS) ou armazenamento de base de dados, devem possuir acesso seguro por meio de comunicação criptografada, bem como a autenticação segura e com garantia de segregação dos dados da MAPS.

Os acessos devem ser controlados por meio de credenciais de acesso individuais fornecidos pelo time de operações, com permissões limitadas de acordo com a função do colaborador ou terceiro.

Plano de Continuidade

A MAPS adota medidas e processos de preparação para desastres, tal como backups, redundâncias e contingências, visando mitigar os riscos associados à perda de dados e interrupções não planejadas. Periodicamente, é feita uma análise em cima da BIA (Business Impact Analysis), para mapear todos os RTOs (Recovery Time Objective) e RPOs (Recovery Point Objective) de todas as ferramentas tecnológicas utilizadas internamente, para estabelecer as contingências para as mesmas.

Os processos de Disaster Recovery, com base na preparação para desastres, são testados anualmente. Também são feitos anualmente treinamentos e testes com todos os colaboradores sobre o Plano de Continuidade de Negócios(PCN), de forma a validar que todos estejam preparados para agir corretamente em caso de incidentes. Tanto os testes dos procedimentos de DR quanto do PCN geram insumos para o CSI elaborar um relatório executivo, indicando pontos de melhoria a serem priorizados e executados.

Gestão de Fornecedores

A MAPS considera a avaliação de risco e classificação dos fornecedores (estratégico, tático, operacional) como parte fundamental de seu escopo institucional.

A contratação de fornecedores se pautará, no que tange à segurança da informação e cibernética, nos seguintes critérios:

- Deverá possuir políticas, programas e procedimentos formais relativos à segurança da informação, que sejam passíveis de auditoria e atualizados periodicamente;
- Deverá possuir plano de resposta a incidentes de segurança cibernética;
- Deverá realizar, em medida adequada, ações de conscientização, educação e formação de segurança de seus colaboradores;
- Caso o item fornecido seja parte de um processo interno da MAPS listado na BIA, o fornecedor deverá possuir preparação e procedimentos de recuperação compatíveis com a criticidade do recurso, de preferência com RTO e RPO definidos.

Controles Criptográficos

Controles criptográficos são utilizados pela MAPS, para proteger as informações segundo os requisitos da sua classificação.

O gerenciamento das chaves de criptografia prevê mecanismos para o armazenamento seguro, geração segura da chave e destruição da chave. As chaves de criptografia devem ser trocadas periodicamente, dependendo da sua frequência de utilização.

EM TRÂNSITO

São dados que estão em movimento, ou seja, estão sendo transferidos ou transmitidos de um local para outro. Isso geralmente ocorre durante a comunicação entre dispositivos ou por meio de redes, como a internet. Sempre

que disponível, deve ser aplicada ao menos um método de criptografia para dados em trânsito.

O uso de criptografia é obrigatório para dados entrando ou saindo da intranet da MAPS. O uso de protocolos não seguros nesses casos é proibido, sendo necessário buscar alternativa técnica.

O uso de criptografia dentro da intranet é fortemente recomendado, devendo ser usado sempre que houver opção disponível.

EM REPOUSO

São os dados que estão armazenados e em repouso em algum dispositivo de armazenamento, como arquivos armazenados no computador do colaborador, informações contidas em um banco de dados da MAPS, entre outros.

Dados confidenciais em repouso devem sempre ser encriptados.

Segurança em Redes

A MAPS estabelece controles tecnológicos para proteger o acesso entre redes. Todos os serviços em redes são acessíveis apenas por VPN. Além do controle de acesso entre as redes, a MAPS protege a informação em trânsito, seguindo os requerimentos da classificação da informação

Os serviços de rede são hospedados em segmento apartado dos usuários, o que restringe o acesso a portas não autorizadas.

Os níveis de segurança (confidencialidade, integridade e disponibilidade) esperados dos serviços de comunicações, devem ser estabelecidos nos contratos firmados com os fornecedores desses serviços.

Os usuários devem manter as credenciais de acesso com política de senha forte, senhas individuais e de uso apenas corporativo, e recomenda-se a atualização de senha com periodicidade mínima de 1x ao ano. Todos os usuários devem manter ativa e fazer uso da autenticação de dois fatores fornecida pela área de Operações de TI.

Licença de Software

O uso de softwares licenciados desempenha um papel fundamental nas operações e no ambiente tecnológico da MAPS.

A aquisição de licenças de software permite que a MAPS tenha acesso legal e autorizado a ferramentas tecnológicas essenciais para suas atividades. Isso não apenas garante o uso correto e ético desses produtos, mas também proporciona suporte técnico, atualizações regulares e recursos de segurança, resultando em um ambiente de trabalho mais seguro e confiável.

Fica estabelecido que:

- Todo equipamento deverá ter o seu sistema operacional devidamente licenciado obedecendo os termos de utilização do fabricante;
- Softwares de uso diário, que não possuírem licenças gratuitas, também deverão obedecer às regras de licenciamento do fabricante;
- Os colaboradores da MAPS só poderão utilizar softwares licenciados e autorizados pelo time de Operações de TI.

Os colaboradores e a área de Operações de TI não possuem autorização para efetuar instalações de softwares não licenciados. Se optarem pela instalação de um software não licenciado, será devidamente rastreado e estarão se responsabilizando pelas penalidades/problemas que tal ação poderá acarretar.

Conscientização sobre Segurança da Informação e Cibernética

Esta Política de Segurança Cibernética deve ser amplamente divulgada no processo de admissão e integração de novos colaboradores pela equipe de Capital Humano.

Programas de conscientização, divulgação e reciclagem do conhecimento da política de segurança cibernética e da Informação devem ser estabelecidos, pelo

Grupo de Segurança da Informação e praticados regularmente, para garantir que todos os colaboradores e terceiros conheçam as diretrizes e responsabilidades relacionadas à segurança das informações.

BYOD (Bring Your Own Device)

É estabelecido pela MAPS em seu escopo institucional como primeiro recurso, que os colaboradores **OBRIGATORIAMENTE** utilizem os equipamentos e acessórios fornecidos pela empresa, os quais são entregues no momento de entrada na empresa. Como opção, a MAPS adere ao modelo BYOD (Bring Your Own Device), modelo em que os colaboradores utilizam seus dispositivos pessoais, para fins de trabalho, desde que os equipamentos atendam aos requisitos estabelecidos pela equipe de Operações de TI relacionados à segurança da informação, cibernética, de hardware e administração da máquina.

Para o uso dos dispositivos, fica estabelecido que:

- O acesso de dispositivos particulares à rede wi-fi da empresa é permitido, desde que utilizados com a autenticação de rede do usuário;
- O funcionário que adotar o uso do BYOD deverá obrigatoriamente devolver o notebook da MAPS caso o tenha.
- A administração, suporte e manutenção a equipamentos particulares **NÃO** é de responsabilidade do time de operações da MAPS, e o colaborador que optar por abrir mão de equipamento da MAPS em favor de um particular assume essa responsabilidade integralmente, sem ônus à MAPS;
- **NÃO** há qualquer garantia quanto à compatibilidade do equipamento próprio do indivíduo com os softwares utilizados pela MAPS e com os recursos de rede (tal como servidor de arquivos, impressora, scanner, VPN etc.);

- A MAPS também **NÃO** se responsabiliza pela instalação de softwares não-licenciados, violação de direitos autorais ou atividades ilegais, como hacking, phishing e práticas correlatas a partir do notebook particular. Em caso de problemas, a MAPS **NÃO** é obrigada a fornecer qualquer tipo de serviço de suporte, podendo neste caso fornecer um equipamento da empresa para o trabalho.

- **NÃO** é permitido o uso de celulares particulares para comunicação com clientes ou fornecedores. Toda comunicação deve ser feita formalmente por meios disponibilizados pela empresa (telefone comercial e e-mail corporativo);

- Estão liberados desta conduta, todos os colaboradores em cargos de confiança, ou que realizam trabalho externo incompatível com a fixação e controle de horário de trabalho;

- Caso o colaborador não more no exterior, deverá seguir o procedimento de solicitação para utilizar equipamento próprio, descrito no portal de processos da MAPS, o qual será submetido à análise, aprovação e autorização para uso;

- O acesso remoto pelo time de Operações será realizado pela ferramenta corporativa conectada remotamente aos dispositivos dos colaboradores.

AVISO: O desvio desta conduta poderá acarretar sanções disciplinares ou administrativas.

4. Responsabilidades

A. GRUPO DE SEGURANÇA DA INFORMAÇÃO

» Representar o compromisso da Gestão da MAPS com a Segurança da Informação e Cibernética;
» Planejar e demandar a implantação de medidas de segurança que atendam aos objetivos desta política;
» Garantir a atribuição dos recursos necessários (financeiros, humanos e tecnológicos) para a implementação da Política de Segurança Cibernética;
» Garantir que todas as normas e diretrizes vigentes na Política de Segurança Cibernética sejam seguidas;
» Propor iniciativas relacionadas à melhoria da Segurança Cibernética da MAPS;
» Promover a divulgação da Política e conscientização sobre Segurança Cibernética a todos os colaboradores e parceiros;
» Avaliar os incidentes de segurança e propor ações corretivas.

B. GRUPO DE COMPLIANCE E GESTÃO DE RISCOS

» Definir diretrizes e estratégias relativas à gestão de riscos e controles internos relacionados a segurança cibernética, bem como planejar e adotar medidas para a implementação de práticas voltadas ao gerenciamento de riscos;
» Acompanhar se as recomendações de melhorias e conformidades foram implementadas.

C. OPERAÇÕES DE TI

» Responsável pela implementação da política de segurança mediante a execução de processos e aplicação dos recursos tecnológicos cabíveis para proteção da infraestrutura utilizada em processos internos da MAPS.
» Administra acessos e permissões de todos os colaboradores de acordo com seus perfis funcionais.
» Garante o estado de contínua preparação para incidentes.
» Monitora e atua na resolução de incidentes.

D. CLOUD

» Responsável pela implementação da política de segurança mediante a execução de processos e aplicação dos recursos tecnológicos cabíveis referentes ao SaaS fornecido pela MAPS a seus clientes.
» Administra acessos e permissões aderentes ao SaaS contratado, provendo acesso aos ambientes contratados aos clientes do MAPS Cloud.
» Garante o estado de contínua preparação para incidentes.
» Monitora e atua na resolução de incidentes.

E. COLABORADORES

» Seguir as normas e diretrizes estabelecidas nesta política.

5. Definições

» **Backup:** é uma cópia de segurança ou duplicata de dados, arquivos ou informações armazenados em um dispositivo ou sistema de computador que é criada com o propósito de restaurar esses dados em caso de perda, corrupção, exclusão acidental, falha do sistema ou outro desastre relacionado à informática.

» **Criptografia:** processo de converter informações legíveis em um formato ilegível, chamado de "texto cifrado", com a finalidade de proteger a confidencialidade, autenticidade e integridade dos dados.

» **Código Malicioso:** código de software que foi criado com a intenção de causar danos, comprometer a segurança de sistemas de computador ou executar ações não autorizadas sem o conhecimento ou consentimento do usuário. Esse código é frequentemente projetado para realizar atividades prejudiciais, como roubo de informações, interrupções do funcionamento de sistemas, extorsão de usuários ou outras ações maliciosas.

- **Grupo de Compliance e Gestão de Riscos:** Grupo que integra o Comitê de Segurança da Informação, Compliance e Gestão de Riscos da MAPS, cujo objetivo é avaliar, monitorar, identificar e expurgar os riscos relevantes do negócio para os objetivos da organização.

- **Grupo de Segurança da Informação:** grupo que integra o Comitê de Segurança da Informação, Compliance e Gestão de Riscos da MAPS, cujo objetivo é propor diretrizes e normas gerais relativas aos temas de segurança da informação e cibernética.

- **Hardware:** refere-se à parte física, tangível, de um sistema de computador. Ele inclui todos os componentes físicos que compõem um computador, desde os dispositivos de entrada e saída até os componentes internos

- **Riscos:** oportunidades ou impedimentos futuros, dotados de grau de incerteza em relação à sua ocorrência, que podem trazer consequências positivas ou negativas, podendo impactar os objetivos gerais e estratégicos da MAPS.

- **Serviço Cloud:** refere-se a um modelo de prestação de serviços de computação pela internet. Em vez de executar aplicativos e armazenar dados em servidores locais ou em hardware pessoal, os serviços de nuvem permitem que as organizações utilizem recursos de computação fornecidos por provedores de nuvem em um ambiente remoto, geralmente através da internet.

- **Software:** é a parte lógica, não tangível, de um sistema de computador. Ele consiste em programas, aplicativos, instruções e dados que direcionam o funcionamento de um computador e permitem que ele execute tarefas específicas.

maps registradora

Rua Afonso Celso, 552 / 6º andar
Vila Mariana / São Paulo / SP / 04119-002
+55 11 5085-7000
contato@mapsregistradora.com.br
www.mapsregistradora.com.br