SUMÁRIO

1. APRESENTAÇÃO

Objetivo

Estabelecer e difundir as Diretrizes da Política de Segurança da Informação visando à orientação quanto ao uso adequado das informações e dos recursos de tecnologia da informação que as suportam, prezando pela sua confidencialidade, integridade e disponibilidade.

Princípios

- Preservar e proteger as informações sob a responsabilidade do IPMMI e suas filiais dos diversos tipos de ameaças e desvios de finalidade em todo o seu ciclo de vida.
- Prevenir e mitigar impactos gerados por incidentes envolvendo a segurança da informação e comunicação.
- Cumprir a legislação vigente no Brasil e demais instrumentos regulamentares relacionados às atividades do IPMMI e suas filiais no que diz respeito à segurança da informação, aos objetivos institucionais e aos princípios de privacidade, morais e éticos.

Campo de Aplicação

A Política de Segurança de Informação se aplica aos colaboradores, prestadores de serviços, clientes, fornecedores e demais que estejam a serviço do IPMMI Administração Corporativa e suas filiais.

2. CONCEITOS E DEFINIÇÕES

Para os efeitos desta política são estabelecidos os seguintes conceitos e definições:

Ativo

Qualquer coisa de propriedade de um indivíduo ou organização que tem valor, sendo ele tangível ou intangível.

Ativo de Informação

Os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso [NC04/IN01/DSIC/GSIPR,2009, p.2].

Titular de dados

É a pessoa física a quem se referem os dados pessoais que são objeto de tratamento.

Recurso de Tecnologia da Informação e Comunicação (TIC)

Todos os equipamentos, instalações e recursos de informação direta ou indiretamente administrados, mantidos ou operados pelos setores e colaboradores. Recursos de informação que incluem todas as informações eletrônicas, serviço de correio eletrônico, mensagens eletrônicas, dados corporativos, documentos, programas ou software que são armazenados, executados ou transmitidos através da infraestrutura computacional do IPMMI e suas filiais, redes ou outros sistemas de informação.

Dados

Dados são partículas de registros quaisquer, como números, confirmações de conforme e não conforme,métricas de uma atividade ou qualquer outro material bruto.

Informação

A informação é uma constatação sólida e comprovada sobre um fato, hipótese ou padrão de comportamento provenientes dos dados. Depois desse processo de captação, tratamento e análise, os dados se tornam informações.

Segurança da informação (SI)

Prioritariamente: preservação da confidencialidade, da integridade e da disponibilidade da informação. Sinteticamente, refere-se à proteção contra o uso ou acesso não autorizado da informação, bem como à proteção contra a negação do serviço a usuários autorizados, ao mesmo tempo em que a confidencialidade, integridade e a disponibilidade da informação são preservadas. Constitui-se, então, de ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações

[IN01/DSIC/GSIPR, 2008, p.2].

Confidencialidade

Garantia de que o acesso à informação seja obtido apenas por pessoas autorizadas, ou seja: propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizado e credenciado [IN01/DSIC/GSIPR, 2008, p.2].

Integridade

Salvaguarda de exatidão e completude da informação e dos métodos de processamento, ou seja: propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental [IN01/DSIC/GSIPR,2008, p.2].

Disponibilidade

Garantia de que usuários autorizados obtenham acesso à informação e aos recursos correspondentes sempre que necessário, ou seja: propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade [IN01/DSIC/GSIPR, 2008, p.2].

Vulnerabilidade

Conjunto de fatores internos ou causa potencial de um incidente indesejado, que podem resultar em risco para um sistema ou organização, os quais podem ser evitados por uma ação interna de segurança da informação [NC04/IN01/DSIC/GSIPR, 2009, p.3].

Ameaça

Conjunto de fatores externos ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização.

3. DISPOSIÇÕES GERAIS

As diretrizes estabelecidas nessa Política de Segurança da Informação devem ser seguidas por

todos os colaboradores, prestadores de serviços, clientes, fornecedores e demais que estejam a serviço do IPMMI e suas filiais, incumbindo a todos a **responsabilidade e o comprometimento com sua aplicação**, seja qual for a forma meio ou recurso relacionado ao IPMMI e suas filiais, será sempre protegida adequadamente de a acordo com essa política.

- Concordar plenamente com as regras e responsabilidades definidas neste documento e demais normais internas do IPMMI sobre o uso dos recursos computacionais.
- Responder por atos que violem as regras de uso dos recursos computacionais, sujeito às penalidades definidas na política de uso desses recursos assim como junto à Gestão de Pessoas.
- Não se fazer passar por outra pessoa ou dissimular sua identidade quando utilizar os recursos computacionais.
- As informações produzidas por usuários internos ou externos, no exercício de suas funções, são patrimônio intelectual IPMMI e suas filiais e não cabe a seus criadores qualquer forma de direito autoral, ressalvando o direito de autoria, se for o caso. É vedada a utilização de patrimônio intelectual do IPMMI e suas filiais em quaisquer projetos ou atividades de uso diverso do estabelecido pela instituição, salvo com autorização específica.
- É vetado o registro e/ou publicação de imagens de serviços ou locais da empresa na internet, haja vista que não se trata de um ambiente que lhe pertence e sim do empregador. Desta forma, o empregado não pode dispor o que não é seu, sob pena de justa causa, conforme artigo 482 da CLT. O empregado deve consultar a empresa se esta lhe concede autorização para tal prática.
- Usar de ética, boa fé e bom senso para com as atividades e uso de quaisquer recursos corporativos.
- Zelar por toda e qualquer informação da empresa contra alteração, destruição, divulgação, cópia e acesso não autorizado.
- Não utilizar os recursos disponíveis para constranger, assediar, prejudicar ou ameaçar qualquer pessoa.
- Não utilizar ferramentas lógicas ou físicas, desenvolvidas para quebrar a segurança dos sistemas de informação.
- Jogos estão terminantemente proibidos.

- Todos os arquivos armazenados nos equipamentos do IPMMI e suas filiais são de domínio do mesmo, podendo ser auditados, independentemente de aviso prévio ao usuário.

4. COMPUTADORES E EQUIPAMENTOS CORPORATIVOS

Esta política deve ser cumprida visando estabelecer os critérios de manuseio, prevenção e responsabilidades sobre o uso dos recursos computacionais, devendo ser aplicado a todos os colaboradores que os utilizem.

São considerados **recursos computacionais**, dentre outros, os equipamentos (hardware), as instalações físicas, os programas de computador (softwares), os serviços que direta ou indiretamente estão relacionados ao processamento, ao armazenamento e à transmissão digital de dados, bem como, qualquer dado acessível por meio desses equipamentos ou programas de computador.

- Fazer bom uso dos equipamentos.
- Todas as estações de trabalho são de propriedade do IPMMI e suas filiais.
- As estações de trabalho estão sendo configuradas seguindo padrões de segurança, cuja atualização será realizada pela equipe de TICP do IPMMI e suas filiais.
- Os usuários têm direitos restritos às estações de trabalho, devendo observar as Políticas de Segurança de TICP.
- É vetado o uso de computadores, laptops e outros dispositivos pessoais conectados à rede corporativa do IPMMI e suas filiais.
- Os recursos de Tecnologia da Informação e Comunicação disponibilizados pelo IPMMI e suas filiais devem ser usados estritamente para seu propósito.

5. MESA LIMPA E TELA LIMPA

Deve ser seguido o princípio estabelecido na Norma ABNT NBR/ISO/IEC 27.001 da Mesa limpa/Tela limpa. Segundo este princípio para se reduzirem os riscos de acesso não autorizado, perda de informações ou danos às informações durante e fora do horário de expediente, deve considerar a adoção de "mesas limpas" para os papéis e mídias de armazenamento removível e, igualmente, “telas limpas”, contra, por exemplo, o perigo de ter um usuário já

autenticado/registrado, porém ausente e com sua sessão de trabalho aberta. Sempre que o colaborador se afastar de seu posto de trabalho é necessário bloquear a tela do computador ou laptop.

A equipe de TI deve implementar o bloqueio automático de tela após no máximo 5 minutos de inatividade, podendo o tempo ser menor de acordo com a área e criticidade das informações da estação de trabalho e usuário que a utilize.

6. IMPRESSORAS

As impressoras do IPMMI e suas filiais são exclusivamente para o desenvolvimento das atividades corporativas. Todas as impressões são monitoradas pelo time de TICP e o uso indevido está sujeito a punições, conforme manual do colaborador.

7. DISPOSITIVOS MÓVEIS

A mobilidade é uma estratégia corporativa, mas esse recurso exige cuidados. O uso dos dispositivos móveis seguindo a Política aqui estabelecida, evitam riscos, possíveis danos e ou exposição indevida da privacidade e integridade do IPMMI e suas filiais.

- Os notebooks são configurados, seguindo padrões de utilização diferenciados para cada segmento, conforme necessidade do suporte prestado.
- Todos os notebooks são de propriedade do IPMMI e suas filiais, que pode alterar sua designação, conforme sua conveniência.
- É vetado o uso de dispositivos de armazenamento portáteis, como Hard Drives e Pen Drives.
- Quando necessário a utilização de mídias removíveis, o usuário deve abrir uma solicitação para o departamento de infraestrutura via canal de chamados de TICP do IPMMI e suas filiais, que irá solicitar aprovações necessárias para liberação temporária do recurso para o usuário específico.

8. INTERNET

O IPMMI e suas filiais fornece acesso à Internet aos usuários de rede e aos recursos

computacionais autorizados. Este acesso deverá ser utilizado exclusivamente como ferramenta de trabalho e usado com responsabilidade, tendo em vista os riscos envolvidos em segurança e produtividade.

- A internet conta com filtros de bloqueio a sites que não são pertinentes ao trabalho realizado pelo IPMMI e suas filiais.
- Toda informação trafegada dentro do IPMMI e suas filiais poderá ser monitorada e vir a ser utilizada para fins de controle.
- É vetado o acesso a redes sociais.
- É expressamente proibido a obtenção, armazenamento, uso ou repasse de conteúdo ilícito como pedofilia, pornografia, apologia às drogas, terrorismo e outros que não estejam em conformidade com o IPMMI.

9. CORREIO ELETRÔNICO E-MAIL

O IPMMI e suas filiais pode disponibilizar uma conta de Correio Eletrônico aos seus colaboradores, conforme necessidade expressa pelo departamento, cargo ou função. O e-mail segue padrão de domínio do IPMMI ou filiais e as regras descritas abaixo.

- Todos os e-mails criados pelo IPMMI e suas filiais são de uso exclusivo para fins empresarial, podendo ser monitorados e auditados conforme a necessidade, sem aviso prévio ao usuário.
- É vetado o uso do e-mail corporativo para fins pessoais, assim como cadastro e divulgação em sites/sistemas, propagandas e anúncios particulares, que não estejam em conformidade com o IPMMI.
- É vetado o uso do e-mail PESSOAL para compartilhamento, armazenamento de arquivos e qualquer outra atividade comercial relacionada ao IPMMI e suas filiais, assim como cadastro em sistemas e sites internos.
- É vetado a veiculação de e-mails com conteúdo ilícito como pedofilia, pornografia, apologia às drogas, terrorismo e outros que não estejam em conformidade com o IPMMI.

10. SOFTWARE

O departamento de TICP do IPMM assegurará que são conhecidas todas as condições aplicáveis ao licenciamento do software e uso pelos utilizadores. É de responsabilidade dos colaboradores seguir as regras abaixo descritas para o melhor uso deste recurso.

- Programas de computador ou software são propriedade intelectual, protegida por Lei no 9.609/1998, que dispõe sobre a proteção da propriedade intelectual de programa de computador, e pela Lei no 9.610/1998 que trata dos direitos autorais. Deve-se considerar que o uso de softwares não licenciados pode prejudicar a segurança dos dados por uma série de razões. Entre elas destacam-se:

  - Desconhecimento da origem: o software pode conter trojans, backdoors ou outros malwares.

  - Eventualmente, para uso destes softwares pode ser preciso desligar mecanismos de proteção ou, então, não fazer uso de determinados mecanismos de segurança.

  - Também deve ser considerado que o uso de software não licenciado é crime.

  - E a penalidade pode chegar a multa proporcional ao valor comercial do software, segundo interpretações baseadas no Art. 56 da Lei9.610/98.

- É vetado o uso de softwares de mensagem instantânea (diferentes do Teams corporativo), como meio de comunicação e armazenamento de informações relacionados ao IPMMI e suas filiais. Exemplo o uso do WhatsApp, Telegram... e outros.
- Toda necessidade de instalação e uso de softwares (externo e interno) diferente dos softwares homologados, devem ser solicitados e comunicados ao departamento de TICP através de chamado. Será feito a avaliação da permissão de uso do mesmo, não cabendo ao usuário tal decisão.

11. SENHA

Todo o colaborador que se faz necessário ter **usuário e senha** para uso em recursos computacionais do IPMMI e suas filiais, mediante aprovação, terá seu acesso liberado pertinente à necessidade do setor/departamento. O IPMMI e suas filiais, concederá os recursos necessários para o desenvolvimento das atividades relacionado aos negócios do IPMMI e suas filiais. Porém

deve ser levado em consideração que:

- A senha de acesso aos recursos computacionais e sistemas do IPMMI e suas filiais, são de uso PESSOAL e INTRANSFERÍVEL. É de responsabilidade do usuário o uso devido para evitar roubo, deturpação das informações e para possibilitar rastreabilidade no processo de controle de acesso.
- Para maior segurança, as senhas de acesso aos equipamentos e sistemas corporativos devem ser alfanuméricas, conter letras números e caractere especial.
- Manter em caráter confidencial, sigiloso pelo próprio colaborador, não sendo permitido anotar em cadernos, agendas, smartphone ou outros recursos.
- Em caso de dúvida sobre o sigilo da senha, o colaborador responsável pelo login e senha deverá solicitar o reset mesmo através da abertura de chamado para o TICP.
- Os colaboradores poderão acessar a rede e os sistemas nos horários de trabalho, podendo ser desconectados fora desse período. Exceções deverão ser solicitadas pelos superiores imediatos através de chamado técnico.
- Em caso de situações comprovadas de acesso e manipulação indevida da informação, o colaborador será sujeito à advertência ou medidas administrativas cabíveis.

12. VIGÊNCIA E VERSÃO

Esta política entra em vigor imediatamente, com prazo de validade indeterminado, portanto, sua vigência se estenderá desde sua publicação, gerando efeitos imediatos, até a sua edição, atualização ou revogação.

Quando se houver necessário, novas versões serão publicadas e divulgadas sistemicamente, introduzindo maturidade à segurança da informação no IPMMI e suas filias.

Histórico

Data	Versão	Natureza da operação	Autor
01/12/2021	01	Elaboração	Paulo Ferreira / Tayse Rosas

13. RESPONSABILIDADE

Esta política é de responsabilidade do departamento de Tecnologia da Informação, Comunicação e Processo (TICP) do IPMMI. Qualquer mudança dessa política deve ser aprovada pelo Conselho de Administração, Diretoria Executiva e departamento de TI do IPMMI.

A alta gestão tem o comprometimento com a melhoria contínua dos procedimentos relacionados com a segurança da informação do IPMMI e suas filiais.

Os casos omissos e as dúvidas surgidas na aplicação do disposto nesta Política, devem ser direcionados ao Gestor do departamento de TICP.