Notas:

1. Garantia de que a informação seja acessada somente por pessoas autorizadas.
2. Garantia de que a informação não seja modificada, acidental ou intencionalmente.
3. Garantia de que as pessoas autorizadas tenham acesso à informação e aos sistemas associados, quando requerido.
4. Garantia de que a informação ou o dado pessoal foi produzido, expedido, modificado ou destruído por uma determinada pessoa física, equipamento, sistema, órgão ou entidade.
5. O incidente de segurança da informação é um único ou vários eventos de segurança da informação, indesejados ou inesperados, com uma probabilidade significativa de comprometer as operações e ameaçar a segurança da informação.

- **Objetivo**: Esta Política de Segurança da Informação ("PSI") tem por objetivo orientar e estabelecer as diretrizes, normas e procedimentos que promovam a segurança das informações, ao tempo que não impeçam nem dificultem os processos de negócio da organização, promovendo:
  - O atingimento dos objetivos da segurança da informação na proteção da confidencialidade[1], integridade[2], disponibilidade[3] e autenticidade[4] da informação, propriedades essenciais da segurança da informação.
  - A garantia da medição do alcance dos objetivos, através dos seguintes indicadores de desempenho: vulnerabilidades externas, atualização de antivírus nas estações de trabalho, acordos de tempo de resposta a incidentes de segurança da informação[5] e configurações seguras de servidores.
  - O compromisso da empresa com a proteção das informações, , incluindo os Dados Pessoais, de propriedade da ou tratadas pela Michelin Connected Fleet, de seus colaboradores e daqueles sob sua tutela.
  - A participação de todos os colaboradores para manter e melhorar continuamente o Sistema de Gestão de Segurança da Informação ("SGSI") adotado;
  - A efetiva divulgação, conhecimento e cumprimento das diretrizes, normas e procedimentos de segurança da informação por colaboradores e partes externas relevantes.
- **Escopo da aplicação**: Esta PSI aplica-se a todos os colaboradores e, quando aplicáveis, partes externas que tenham acesso às informações e aos Dados Pessoais de propriedade da ou tratados pela Michelin Connected Fleet, onde quer que estejam alocados e independentemente do método de armazenamento e acesso
- **Revisão e aprovação**: Esta política deve ser analisada criticamente ao menos uma vez ao ano e revisada pela área de Segurança da Informação sempre que for necessário. Novas versões desta política devem ser avaliadas e aprovadas pelo Comitê Executivo de Segurança da Informação e Privacidade ("Comitê"). Após a aprovação, a nova versão será publicada e comunicada pela área de Segurança da Informação a todos os colaboradores e partes externas relevantes.

DIRETRIZES GERAIS DA SEGURANÇA DA INFORMAÇÃO:

I. A responsabilidade pela segurança da informação é de todos os colaboradores da organização, assim como de partes externas relevantes.

II. A conscientização sobre segurança deve garantir que os funcionários estejam cientes de como manter as informações seguras e protegidas.

III. Um programa contínuo de conscientização está estabelecido e mantido para garantir que a conscientização da equipe seja atualizada conforme necessário.

IV. A conscientização deve tornar os usuários cientes de suas responsabilidades para manter controles de acesso eficazes, por exemplo, escolhendo senhas fortes e mantendo sua confidencialidade.

V. A preocupação com a segurança da informação deve estar presente em todas as atividades da organização, em especial nas tomadas de decisão.

VI. A Michelin Connected Fleet estabelece e mantém um Sistema de Gestão da Segurança da Informação, adotando as melhores práticas de mercado e em conformidade com a legislação, normas e regulamentos aplicáveis.

VII. O uso dos ativos de informação da organização deve ser feito de maneira ética e profissional por todos;

VIII. Os ativos de informação devem estar íntegros e disponíveis, sempre que demandados por entidade autorizada.

IX. O descumprimento desta política e de outras políticas, normas, guias e procedimentos que a suportam constitui incidente de segurança da informação.

X. Todo e qualquer Incidente de segurança da informação deve ser comunicado e tratado, podendo implicar em medidas disciplinares previstas no Código de Ética e na aplicação de sanções previstas em contrato ou na legislação vigente. Papéis, responsabilidades e procedimentos a serem seguidos são documentados nos procedimentos de Gerenciamento de segurança da informação.

Esta Política está sujeita a atualizações periódicas. Consulte sempre a versão atual.