POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

1. Objetivo

O objetivo desta Política é definir os princípios e as orientações relacionadas à segurança da informação, com o intuito de resguardar a organização, seus clientes e o público em geral. São partes integrantes dessa Política de Segurança da Informação (PSI) a Política de Privacidade e Proteção de Dados e o Plano de resposta a incidentes de segurança.

2. Abrangência

Esta Política aplica-se a administradores, funcionários, estagiários, fornecedores, prestadores de serviços e parceiros da Catavento Pesquisas LTDA (Empresa)

3. Conceitos

A segurança da informação é aqui caracterizada pela preservação dos seguintes conceitos:

- **confidencialidade**: garantia de que a informação somente possa ser acessada por pessoas autorizadas, pelo período necessário;
- **disponibilidade:** garantia de que a informação esteja disponível para as pessoas autorizadas quando se fizer necessária; e
- **integridade:** garantia de que a informação esteja completa, exata, íntegra e que não tenha sido modificada ou destruída indevidamente, de maneira não autorizada ou acidental durante o seu ciclo de vida.

4. Responsabilidades

A informação é um recurso valioso de extrema importância para a Empresa, essencial para o êxito de suas operações, e, portanto, requerendo uma proteção adequada.

Segurança da informação envolve a implementação de medidas para salvaguardar a propriedade, confidencialidade, disponibilidade e integridade dos dados, em todas as suas formas e meios de armazenamento - físicos ou digitais - frente às diversas ameaças existentes. Isso visa evitar qualquer uso indevido, impróprio, ilegal ou em desacordo com as políticas e procedimentos internos. Nesse sentido, é crucial seguir as orientações fornecidas abaixo.

4.1. Propriedade, registro e classificação da informação

As informações geradas pelos colaboradores abrangidos por esta Política, independentemente do formato (físico ou digital), são propriedade exclusiva da Empresa. Da mesma forma, as informações fornecidas à empresa por terceiros, de maneira autorizada, também são de sua propriedade, devendo ser utilizadas única e exclusivamente para atender aos objetivos do negócio. É imprescindível atribuir as informações a proprietários

designados formalmente, responsáveis pela autorização de acesso às informações sob sua responsabilidade.

Para garantir a segurança da informação, é necessário que as informações sejam adequadamente protegidas e rotuladas, seguindo rigorosamente as diretrizes estabelecidas para a segurança da informação. Nesse sentido, deve ser utilizado o modelo de registro das operações de tratamento de dados pessoais para agentes de tratamento de pequeno porte (ATPP) conforme Resolução CD/ANPD Nº 2. Essa prática assegura o cumprimento das políticas estabelecidas e a preservação da integridade, confidencialidade e disponibilidade das informações.

4.2. Controle de Acessos e Identidades

A gestão dos acessos aos recursos informacionais e ambientes tecnológicos da Empresa requer uma meticulosa supervisão em consonância com a sua classificação, sendo sujeita a revisões periódicas. Tal prática visa a disponibilização restrita aos indivíduos autorizados, conferindo-lhes apenas os privilégios necessários para o desempenho eficaz de suas incumbências.

4.3. Eliminação de Dados

O processo de descarte de informações deve ser executado mediante a aplicação de medidas que inviabilizem qualquer possibilidade de reconstrução, de acordo com as exigências específicas do suporte, seja físico ou digital. O procedimento de eliminação deve levar em consideração os prazos mínimos estipulados por normas legais ou regulatórias, assim como a imprescindibilidade da informação para os propósitos do negócio ou da área, adotando o critério mais extenso quando aplicável.

4.4. Parcerias com Fornecedores e Entidades Externas

Os contratos estabelecidos com as entidades fornecedoras de serviços que detêm acesso às informações, sistemas e/ou ambientes da Empresa devem incorporar cláusulas que garantam a adesão rigorosa às normativas de segurança da informação, além de prever penalidades diante de eventuais descumprimentos.

5. Responsabilidades

5.1. Dos colaboradores abrangidos por esta política:

- Cumprir integralmente as regras estabelecidas por esta política, pela Política de Privacidade e Proteção de Dados e o Plano de resposta a incidentes de segurança.
- Garantir a efetiva proteção das informações contra acessos não autorizados, modificações, destruição ou divulgação não consentida.
- Garantir que as informações e dados pertencentes à Empresa não sejam divulgados a terceiros, a menos que haja autorização por escrito da direção.

- Abster-se de discutir, citar ou compartilhar assuntos confidenciais em ambientes públicos ou expostos, incluindo comentários e opiniões em redes sociais.
- Não compartilhar informações confidenciais de qualquer tipo.
- Observar e cumprir rigorosamente as leis e normas que regulamentam a propriedade intelectual.

5.2. Da direção da empresa

- Reforçar e orientar a equipe quanto às práticas e processos essenciais de segurança da informação.
- Estabelecer normas claras relacionadas à propriedade e uso da informação.
- Implementar e monitorar medidas eficazes para a gestão de acessos e identidades.
- Estabelecer procedimentos robustos para garantir a segurança no acesso a sistemas.
- Assegurar a inclusão de cláusulas específicas nos contratos com empresas prestadoras de serviços que assegurem o cumprimento dessa Política.
- Estabelecer penalidades claras em caso de descumprimento das normas de segurança e desta política.

6. Disposições finais

O disposto acima se aplica, imediatamente, para toda a Empresa, a partir da publicação da presente Política.

Três Coroas, 01 de março de 2024.