POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CYBER SECURITY

1. INTRODUÇÃO

Aqui na **Vantico** desenvolvemos uma nova metodologia para execução de testes de segurança (Pentests) sob demanda e totalmente escalável. Assim, elaboramos esta Política de Segurança da Informação e Cyber Security (Política) para reafirmar o compromisso que temos com a adoção das melhores práticas de segurança da informação e proteção dos dados dos nossos clientes.

2. OBJETIVO

O objetivo desta Política é formalizar os conceitos e as diretrizes da Segurança da Informação e Cyber Security da **Vantico** que visam à proteção dos ativos de Informação, de modo garantir a confidencialidade, integridade e disponibilidade das informações.

3. DEFINIÇÕES

Para os fins desta Política, serão adotadas as seguintes definições:

- **Informação**: reunião ou conjunto de dados e conhecimentos resultante do processamento, manipulação e/ou organização de dados, de tal forma que represente uma modificação (quantitativa ou qualitativa) no conhecimento do sistema (humano ou máquina) que a recebe;

- **Segurança da Informação**: conjunto de ações e controles com objetivo de garantir a preservação dos aspectos de confidencialidade, integridade, disponibilidade, autenticidade e conformidade das informações, contribuindo para o cumprimento dos objetivos estratégicos da **Vantico**;

- **Confidencialidade**: as informações somente devem ser divulgadas a indivíduos, entidades ou processos autorizados;

- **Integridade**: salvaguarda da exatidão da informação e dos métodos de processamento;

- **Disponibilidade**: sempre que necessário, as pessoas autorizadas devem obter acesso à informação e aos ativos correspondentes;

- **Conformidade**: cumprimento de um requisito legal ou regulatório relacionado à administração das empresas, dentro de princípios éticos e de conduta estabelecidos pela Alta Administração da **Vantico**;

- **Incidente de Segurança da Informação**: evento decorrente da ação de uma ameaça que explora uma ou mais vulnerabilidades e que afete algum dos aspectos da segurança da informação: confidencialidade, integridade ou disponibilidade;

- **Risco de Segurança da Informação**: riscos associados à violação da confidencialidade, integridade e disponibilidade das informações da **Vantico** nos meios físicos e digitais.

4. PÚBLICO-ALVO

Esta política se aplica a todos os usuários da informação da **Vantico**, incluindo qualquer indivíduo ou organização que possui ou possuiu vínculo com a **Vantico**, tais como colaboradores, prestadores de serviço, que possuíram, possuem ou virão a possuir acesso às informações da **Vantico** e/ou fizeram, fazem ou farão uso de recursos computacionais compreendidos na infraestrutura **Vantico**.

5. DIRETRIZES GERAIS

A **Vantico** visa estabelecer princípios e diretrizes para assegurar a confidencialidade, integridade e disponibilidade dos dados e dos sistemas de informação utilizados, garantindo a proteção adequada dos ativos e dos dados. Tais medidas garantem, também, a identificação, proteção, detecção, resposta e recuperação de eventos em casos de eventual incidente de segurança.

6. PRINCÍPIOS DA SEGURANÇA DA INFORMAÇÃO

Nosso compromisso com o tratamento adequado das informações da **Vantico**, clientes e público em geral está fundamentado nos seguintes princípios:

- **Confidencialidade**: garantir que a informação não estará disponível ou divulgada a indivíduos, entidades ou aplicativos sem autorização. Em outras palavras, é a garantia do resguardo das informações dadas pessoalmente em confiança e proteção contra a sua revelação não autorizada.

- **Integridade**: garantir que a informação não tenha sido alterada em seu conteúdo e, portanto, é íntegra, autêntica, procedente e fidedigna. Uma informação íntegra é uma informação que não foi alterada de forma indevida ou não autorizada.

- **Disponibilidade**: permite que a informação seja utilizada sempre que necessário, estando ao alcance de seus usuários.

7. CICLO DE VIDA DA INFORMAÇÃO

Para efeito desta política, será considerado o seguinte ciclo de vida da informação:

- **Manuseio**: é a etapa onde a informação é criada e manipulada.

- **Armazenamento**: consiste na guarda da informação, seja em um banco de dados, em um papel, em mídia eletrônica externa, entre outros.

- **Transporte**: ocorre quando a informação é transportada para algum local, não importando o meio no qual ela está armazenada.

- **Descarte**: essa fase refere-se à eliminação de documento impresso (depositado na lixeira e/ou mantido em empresa de armazenagem), eliminação de arquivo eletrônico ou destruição de mídias de armazenamento (por exemplo, CDs, DVDs, disquetes, pen-drives).

8. CLASSIFICAÇÃO DA INFORMAÇÃO

A classificação das informações deve ser avaliada em razão do teor do conteúdo, relevância do conhecimento externo e pelos elementos intrínsecos do documento. O acesso, divulgação e tratamento do documento (físico ou digitalizado), dado ou informação da **Vantico**, são restritos aos colaboradores da **Vantico** que tenham necessidade de conhecê-los em razão de suas atividades profissionais, pautados pela regulamentação existente e pelos princípios de pertinência, utilidade e relevância.

Toda informação de uso corporativo deve ser classificada de acordo com o grau de sigilo para o negócio da empresa, considerando-se os três níveis descritos a seguir:

- **Confidencial**: É o mais alto grau de sigilo, aplicado às informações de caráter estratégico e que devem ser manuseadas por um grupo restrito de usuários. O acesso não autorizado a essas informações pode ter consequências críticas para o negócio, causando danos estratégicos à imagem da empresa.

- **Restrito**: São informações específicas para uso interno, com circulação exclusiva e irrestrita dentro da empresa. Estas informações podem estar disponíveis a todos os colaboradores da **Vantico** e prestadores de serviços, devendo ser utilizadas somente para as atividades da **Vantico**. Essas

informações, mesmo sendo de circulação livre dentro das empresas, não devem ser divulgadas para entidades externas sem os devidos cuidados, incluindo, quando necessário, a assinatura de acordos de confidencialidade ou de autorização formal previamente avaliada pela alçada responsável pela informação ou documento em questão.

- **Público**: São informações de circulação livre e domínio público. Esse tipo de informação não exige controles ou restrições de segurança para seu acesso ou guarda.

PAPÉIS E RESPONSABILIDADES

9. GERÊNCIA DE SEGURANÇA DA INFORMAÇÃO

- Conduzir a Gestão e Operação da segurança da informação, tendo como base esta política e demais resoluções;
- Identificar e avaliar as principais ameaças à segurança da informação, bem como propor e, quando aprovado, implantar medidas corretivas para reduzir o risco;
- Tomar as ações cabíveis para se fazer cumprir os termos desta política;
- Realizar a gestão dos incidentes de segurança da informação, garantindo tratamento adequado.

10. GESTORES DA INFORMAÇÃO

- Gerenciar as informações geradas ou sob a responsabilidade da sua área de negócio durante todo o seu ciclo de vida, incluindo a criação, manuseio e descarte conforme as normas estabelecidas pela Vantico;
- Identificar, classificar e rotular as informações geradas ou sob a responsabilidade da sua área de negócio conforme normas, critérios e procedimentos adotados pela **Vantico**;
- Periodicamente revisar as informações geradas ou sob a responsabilidade da sua área de negócio, ajustando a classificação e rotulagem das mesmas conforme necessário;
- Autorizar e revisar os acessos à informação e sistemas de informação sob sua responsabilidade;
- Solicitar a concessão ou revogação de acesso à informação ou sistemas de informação de acordo com os procedimentos adotados pela **Vantico**.

11. USUÁRIOS DA INFORMAÇÃO

- Ler, compreender e cumprir integralmente os termos da Política Geral de Segurança da Informação, bem como as demais normas e procedimentos de segurança aplicáveis;
- Encaminhar quaisquer dúvidas e/ou pedidos de esclarecimento sobre a Política Geral de Segurança da Informação, suas normas e procedimentos a Gerência de Segurança da Informação;
- Comunicar à Gerência de Segurança da Informação qualquer evento que viole esta Política ou coloque/possa vir a colocar em risco a segurança das informações ou dos recursos computacionais da Vantico;
- Assinar o Termo de Uso de Sistemas de Informação da **Vantico**, formalizando a ciência e o aceite integral das disposições da Política Geral de Segurança da Informação, bem como as demais normas e procedimentos de segurança, assumindo responsabilidade pelo seu cumprimento;
- Responder pela inobservância da Política Geral de Segurança da Informação, normas e procedimentos de segurança, conforme definido no item sanções e punições.

12. GESTÃO DE ACESSO

O acesso a sistemas, recursos e outros ativos de informação deve ser concedido mediante a uma autenticação válida e baseado em:

- Necessidade de negócio;
- O princípio do menor privilégio;
- Segregação de funções.

Os acessos devem ser gerenciados através de um ciclo de vida desde a criação até a desativação, incluindo revisões periódicas quanto à precisão e adequação.

A composição das senhas deve seguir os requisitos de complexidade e ser únicas. Não devem ser reutilizadas, compartilhadas, armazenadas em arquivos ou escritas em qualquer lugar.

Ativos de informação considerados críticos, que armazenem e/ou processem informações sensíveis, devem ser restringidos às áreas segregadas da rede, com controle de acesso apropriado.

13. AUDITORIA

Logs e trilhas de auditoria devem ser habilitados em ambientes de produção, protegidos de acessos e alterações não autorizados e registrar:

- Que atividade foi executada;
- Quem executou a atividade;
- Quando a atividade foi executada;
- Onde a atividade foi executada.

14. CRIPTOGRAFIA

Assegurar o uso efetivo e adequado da criptografia para proteger a confidencialidade, autenticidade e/ou a integridade da informação.

Algoritmos criptográficos devem ser aplicados conforme a necessidade em dados em repouso, em trânsito e/ou em uso.

15. MONITORAMENTO

Ferramentas e processos para monitorar e impedir que informações sensíveis deixem o ambiente interno de uma organização sem autorização devem estar implementados.

Soluções e/ou processos que permitam a prevenção, detecção, e identificação de ataques a componentes da infraestrutura da **Vantico** devem estar implementados.

A utilização dos recursos deve ser monitorada e ajustada e as projeções serem feitas para necessidades de capacidade futura para garantir o desempenho requerido do sistema

16. VULNERABILIDADES

Um processo de gerenciamento do ciclo de vida de vulnerabilidades, desde a identificação até a remediação, incluindo diretrizes para documentação, emissão de relatórios e divulgação deve estar implementado.

Informações sobre vulnerabilidades técnicas dos sistemas de informação em uso, sejam obtidas em tempo hábil, com a exposição da organização a estas vulnerabilidades avaliadas e tomadas as medidas apropriadas para lidar com os riscos associados

17. CÓDIGO MALICIOSO

Assegurar que as informações e os recursos de processamento da informação estão protegidos contra códigos maliciosos.

Soluções de software anti-malware de detecção, prevenção e recuperação ou controles equivalentes devem estar implementadas para proteger o ambiente da **Vantico**.

18. BACKUP

Cópias de segurança das informações, softwares e das imagens do sistema, devem ser efetuadas e testadas regularmente conforme a política de geração de cópias de segurança definida.

19. DESENVOLVIMENTO DE SOFTWARE

Durante o ciclo de vida de desenvolvimento de software, requisitos de segurança devem ser aplicados para garantir a confidencialidade, integridade e disponibilidade das informações.

Deve ser feita uma avaliação de segurança antes da implementação de qualquer nova tecnologia, ferramenta ou solução em produção.

20. INCIDENTE DE SEGURANÇA CIBERNÉTICA

Assegurar um enfoque consistente e efetivo para gerenciar os incidentes de segurança da informação, incluindo a comunicação sobre fragilidades e eventos de segurança da informação.

O consumo e compartilhamento de informações de incidentes e ameaças com outras instituições locais e globais deve ser feito por canais seguros.

21. TREINAMENTO E CONSCIENTIZAÇÃO

Treinamentos de conscientização devem ser obrigatórios e realizados anualmente, apresentando os princípios de segurança da informação para auxiliar os funcionários a reconhecer situações de risco e agir corretamente.

22. ATUALIZAÇÕES

A Política de Segurança Cibernética e demais políticas devem ser revisadas, no mínimo, a cada dois anos.

23. COMUNICAÇÃO

Em caso de dúvida, questão ou preocupação em relação a esta Política, entre em contato através de **security@vantico.com.br**.

24. REVISÕES

Versão	Data	Revisão	Aprovação	Conteúdo Revisado
1.0	15/01/2023	Kaique Bonato	Diretoria	Criação do documento
1.1	09/06/2023	Kaique Bonato	Diretoria	Atualização completa das sessões e layout
1.2	25/03/2024	Kaique Bonato	Diretoria	Atualização de layout e remoção de itens desatualizados

25. INFORMAÇÕES DE CONTROLE

Versão	Código do Documento	Área	Status	Confidencialidade
1.2	POL.SI.001	Segurança	PUBLICADO	PÚBLICO