Política de Segurança da Informação e Cibernética

Sumário

1. Introdução

Esta política define as diretrizes e princípios para garantir a segurança da informação e cibernética em nossa organização. Ela se aplica a todos os colaboradores, sejam sócios ou funcionários, consultores e terceiros que lidam com as informações da empresa.

Cabe ressaltar que são três óticas tratadas sobre o tema para nosso modelo de negócios: envolvendo as informações processadas por nossas aplicações, informações circuladas de nossos clientes e informações de nossa exclusiva utilização.

Informações processadas em nossas aplicações

Como o modelo de negócios principal é a implantação da aplicação e banco de dados na infraestrutura do cliente, as iniciativas dependem também do ambiente técnico do próprio cliente, podendo a B3Bee contribuir com o atendimento às solicitações de implementação técnica sugeridas para funcionamento da aplicação com maior nível de segurança.

Informações circuladas de nossos clientes

Para a prestação de serviços de consultoria circulando informações de clientes se necessário, além das iniciativas descritas a seguir, são detalhados os documentos de ‘Política de manuseio de informações de clientes’ e ‘Política de Uso de Computadores e Segurança de Informações’.

Informações exclusivas da B3Bee

Aplicam-se todas as iniciativas descritas a seguir para efeito de quaisquer informações internas e de posse única e exclusiva da B3Bee, tais como documentações e códigos-fontes, além das recomendações na já citada ‘Política de Uso de Computadores e Segurança de Informações’.

2. Objetivo

O objetivo desta política é proteger as informações contra todas as ameaças, sejam elas internas ou externas, deliberadas ou acidentais, para garantir a continuidade do negócio e minimizar danos a todos os envolvidos nas atividades da empresa.

3. Segurança da Informação

3.1. Princípios da Segurança da Informação: A segurança da informação em nossa organização é baseada nos princípios de Confidencialidade, Integridade e Disponibilidade:

- Confidencialidade: As informações são protegidas contra acesso indevido e divulgação não autorizados.
- Integridade: As informações são protegidas contra alterações não autorizadas, e a precisão e completude das informações são mantidas.
- Disponibilidade: As informações estão disponíveis e acessíveis para uso quando necessário. E seguindo a Política de Backup para manter esse princípio ativo.

3.2. Classificação da Informação: Toda informação deve ser classificada em relação ao seu valor, requisitos legais, sensibilidade e criticidade para a organização.

3.3. Gestão de Acessos: O processo de concessão, revisão e revogação de acessos deve ser documentado e analisado criticamente. Tanto para colaboradores internos, quanto externos.

4. Segurança Cibernética

4.1. Proteger as redes e sistemas contra atividades maliciosas e acesso não autorizado.

4.2. Monitorar e responder a incidentes de segurança cibernética de maneira rápida e eficaz.

4.3. Manter todos os sistemas, softwares e equipamentos atualizados com as mais recentes atualizações e práticas de segurança.

4.4. Realizar avaliações regulares de risco cibernético para identificar e mitigar vulnerabilidades potenciais.

4.5. Garantir a continuidade dos negócios em caso de um incidente de segurança cibernética significativo através de um plano de recuperação de desastres.

4.6. Promover a conscientização e a educação em segurança cibernética entre todos os funcionários e terceiros.

5. Responsabilidades

Todos os colaboradores são responsáveis por aderir a esta política. A violação desta política pode resultar em ação disciplinar prevista na política de conduta ética (v2).

Canal de relato de vulnerabilidades: Todos os colaboradores podem relatar vulnerabilidades identificadas encaminhando e-mail para o endereço suporte@b3bee.com.br (v2).

Quanto ao software licenciado aos clientes (v2)

- Respeitamos a política e recursos computacionais de segurança cibernética da instituição financeira onde o sistema estiver instalado (on premise), ajustando o software à versão, recursos e práticas por eles solicitados, uma vez justificados e/ou evidenciados por softwares de verificação de vulnerabilidades.
- Adequamos e parametrizamos todos os recursos computacionais disponíveis para aumentar a segurança cibernética disponibilizados pelos servidores contratados para armazenamento na nuvem (SAAS), bem como limitando a oferta de sistemas nessa modalidade, cujos dados não possuam dados pessoais ou sensíveis de clientes ou dados sensíveis à instituição financeira.
- Ajustamos o processo de conexão do usuário aos sistemas (login) conforme a política de segurança de acesso a sistemas de cada instituição financeira, tais como SSO e/ou lista unificada de senhas, AD por exemplo (v3).
- Adotamos práticas de desenvolvimento recomendadas em https://owasp.org/www-project-top-ten/ a partir do qual é feita análise de qualidade de implementação dos sistemas.
- Analisamos o código de programação via Sonaqube (v3).

- Periodicamente aplicamos scan via ferramenta ZAP (Zed Attack Proxy), conforme o link https://www.zaproxy.org/ (v3)

Quanto às práticas internas (v2)

- Adotamos e seguimos os procedimentos internos para reduzir invasões e acessos não autorizados aos computadores dos colaboradores da B3Bee em política específica de Uso de Computadores e Segurança da Informação.
- Adotamos o descredenciamento de colaboradores imediatamente após seu desligamento operacional da B3Bee, incluindo revogação de login e senha de acesso aos sistemas de produção e acesso físico às instalações, sendo necessária a partir de então, autorização e acompanhamento por algum responsável pertencente ao quadro funcional da empresa.

6. Histórico

Versão	Data	Autor	Descrição
1	27/07/2023	Comitê de TI	Criação
2	19/01/2024	Yoshio	Referência à política disciplinar da política de conduta ética, formalização do canal de relato de vulnerabilidades e detalhamento de responsabilidades migradas da política de conduta ética (v2).
3	29/01/2024	Yoshio	Atualização pelo acréscimo de novos tópicos já adotados (v3).