1. OBJETIVO

Este documento define os princípios básicos para garantir a proteção das informações da Sistemas & Informação.

2. ABRANGÊNCIA

Esta Política se aplica a todas as informações criadas, recebidas, armazenadas, processadas, transmitidas ou impressas com o auxílio de qualquer sistema, meio de transmissão ou de armazenamento.

No âmbito dessa Política estão todos os colaboradores da Sistemas & Informação, sem exceção, bem como todos os outros indivíduos que direta ou indiretamente utilizam ou suportam os sistemas, infraestrutura ou informações da Sistemas & Informação.

3. VIGÊNCIA

Essa política passa a vigorar a partir da data da publicação.

4. DEFINIÇÕES

Confidencialidade: garantir que as informações sejam acessadas somente por aqueles expressamente autorizados, devendo ser protegidas do conhecimento alheio.

Integridade: garantir que as informações estejam protegidas de modificações, manipulações ou reproduções não autorizadas.

Disponibilidade: garantir que todas as informações e serviços importantes ao negócio estejam disponíveis, sempre que necessário, a pessoas e processos autorizados.

Controle: medida de segurança adotada pela S&I para o tratamento de um risco específico.

Incidente de Segurança da Informação: um incidente de segurança da informação é indicado por um simples ou por uma série de eventos indesejados ou inesperados, que tenham uma grande probabilidade de comprometer as operações do negócio e ameaçar a segurança das informações.

Malware: termo em inglês para Software Malicioso, de forma genérica. Inclui as categorias de *spywares*, vírus e *Worms,* entre outros.

Risco: combinação da probabilidade de um evento e de suas consequências.

Segurança da informação: a preservação das propriedades de confidencialidade, integridade e disponibilidade das informações.

5. DOCUMENTOS RELACIONADOS

MAN-001 – Manual do Sistema de Gestão de Segurança da Informação

POL.004 – Política de Desenvolvimento Seguro

6. DIRETRIZES

6.1. Política de Segurança da Informação

" Garantir a satisfação dos nossos clientes e prover a melhoria contínua dos processos e serviços de tecnologia considerando: Confidencialidade, integridade e disponibilidade das informações das partes interessadas."

6.2. Gestão de Segurança da Informação

De forma geral, a Sistemas & Informação baseia sua estratégia de segurança da informação nas exigências e boas práticas de mercado e em requisitos definidos na Norma Internacional de Gestão de Segurança da Informação – ISO 27001/2013.

A implementação de mecanismos e controles de segurança deve ser justificada com base no valor associado às informações envolvidas e ao impacto oriundo da eventual perda dessas informações.

Os registros de auditoria dos acessos e alterações das informações críticas devem ser devidamente mantidos e tais registros devem possibilitar a identificação de qualquer operação ou alteração não autorizada.

Devem ser priorizadas medidas preventivas ao contrário de controles reativos e, sempre que possível, as medidas de segurança devem ser atendidas através de soluções técnicas que não dependam de processos manuais ou que não estejam sujeitas a erros humanos.

7. DISPOSIÇÕES FINAIS

O presente documento em conjunto com as Políticas e Procedimentos deve ser lido e interpretado pelos colaboradores.

Esta Política, bem como os demais documentos que a complementam encontram-se disponíveis para consulta a qualquer tempo através do servidor do Discord da Sistemas & Informação, ou, em caso de indisponibilidade, podem ser solicitadas à área de segurança da informação.

Qualquer dúvida relativa a esta Política deve ser encaminhada à área de segurança da informação por meio do endereço eletrônico: sgi@sistemaseinformacao.com.br.

8. REVISÃO, ATUALIZAÇÃO E CONSCIENTIZAÇÃO DOS COLABORADORES

Esta Política deverá ser revisada no mínimo uma vez ao ano. Todos os outros documentos que derivam ou ampliam a presente Política deverão ser revisados da mesma forma.

Toda vez que a Política for revisada e/ou alterada, a área de segurança da informação deverá providenciar um treinamento para conscientizar todos os colaboradores e áreas da Sistemas & Informação, sem qualquer exceção.

9. RESPONSABILIDADES

9.1. Proprietário das Informações

É responsável por determinar os usuários da informação recém gerada, identificar o nível de sigilo

adequado, e ainda por aplicar as medidas de segurança que ofereçam a proteção adequada às informações de sua propriedade.

9.2. Usuário das informações

É responsável por zelar pelas informações que cria, retém ou acessa sempre observando as recomendações desta Política e outros documentos que a complementam. Também é responsável por cumprir todas as medidas relacionadas ao uso de informações e sistemas associados. Todos os usuários devem ser informados periodicamente sobre as políticas e procedimentos em vigor, devendo receber treinamento sempre que necessário e comunicar qualquer incidente de segurança da informação à área responsável.

9.3. Gerentes de Projeto

São responsáveis por considerar as recomendações de segurança da informação como parte dos requisitos do projeto durante o ciclo de vida do desenvolvimento de sistemas. São responsáveis por garantir a implementação de segurança de acordo com os requisitos previamente definidos antes que o respectivo sistema seja disponibilizado em ambiente de produção. Também são responsáveis por manter documentadas as recomendações de segurança junto à documentação existente do projeto e ao desenho dos respectivos sistemas.

9.4. Segurança da Informação

É responsável pela implementação da Política de Segurança da Informação e demais documentos, assim como dos respectivos processos e mecanismos. São também responsabilidades do Departamento de Segurança da Informação: Implementar a Gestão de Segurança da Informação; Analisar e fazer recomendações de segurança na infraestrutura e no desenvolvimento de sistemas; revisar e atualizar esta Política e suas respectivas Normas; administrar o programa de Conscientização de Segurança da Informação; verificar periodicamente o cumprimento da Política e a aderência às Normas de Segurança; Coordenar a investigação de incidentes.

É responsável por definir as medidas adequadas para a identificação de ofensas à Política de Segurança da Informação e seus documentos derivados, além de qualificar tais ofensas quanto ao seu nível de criticidade. É responsável ainda por garantir que todas as violações serão punidas e que tais punições serão comunicadas a todos os colaboradores.

- Garantir que novas modalidades de códigos maliciosos são adequadamente investigadas, tratadas e protegidas pela ferramenta corporativa adotada pela Sistemas & Informação;
- Garantir a existência de iniciativas para divulgação sobre informações de ameaças, códigos maliciosos e medidas de proteção para os usuários da Sistemas & Informação.

10. HISTÓRICO DE ALTERAÇÕES

VERSÃO	DATA	NOME	AÇÃO (Elaboração, Revisão, Atualização, Aprovação)	CONTEÚDO
1.0	14/03/2022	Lucas Giacomini Duarte	Elaboração	Primeira versão
		Mário Seixas	Aprovação	