Política	**Data da última atualização**
Segurança da Informação e Cibernética	25/05/2020
Área Responsável	**Versão**
Segurança da Informação	R01

ÍNDICE

1. Objetivos

A Política de Segurança da Informação e Segurança Cibernética da Guide Investimentos tem como objetivo garantir a aplicação de princípios e diretrizes para utilização das melhores práticas de governança para proteção das Informações da empresa, de seus colaboradores, de seus clientes e do público em geral.

Deve estabelecer as práticas para assegurar a confidencialidade, integridade e disponibilidade das informações, além do cumprimento de requisitos regulatórios e operacionais e proteger a empresa de riscos de imagem e legais.

1.2 Segurança da Informação

A Segurança da Informação é obtida a partir da implementação de políticas, processos, procedimentos, e soluções tecnológicas. Os controles de Segurança da Informação devem ser definidos, implementados, monitorados, avaliados e melhorados continuamente.

Convém que isto seja feito em conjunto com outras condutas e processos de gestão, como:

- Cumprir com requisitos legais e regulatórios;
- Avaliar ameaças atuais e futuras ao negócio;
- Proteger informações sensíveis;
- Desenvolver sistemas e serviços com Segurança;
- Agir de maneira profissional e ética.

A Segurança da Informação se baseia nos seguintes pilares fundamentais:

- **Confidencialidade:** garante que a informação estará acessível apenas a pessoas autorizadas. A principal maneira de mantê-la assim é por meio de autenticação, controlando e restringindo o acesso, e impondo limitações de acesso aos dados sigilosos.
- **Integridade:** mede a exatidão da informação e seus métodos de modificação, manutenção e validade. Há perda de integridade quando a informação é alterada indevidamente ou quando não se pode garantir que a informação é a mais atualizada.
- **Disponibilidade:** garante que a informação esteja disponível sempre que for necessário para as pessoas autorizadas.

- **Autenticidade:** tem a finalidade de identificar e registrar o usuário que está realizando o envio ou modificação da informação, de modo que modificações de dados sejam devidamente documentadas.
- **Legalidade**: deve garantir que o uso de recursos de tecnologia e telecomunicação deve estar de acordo com as leis vigentes.

2. Propriedade Intelectual

Todas as informações, artefatos de tecnologia, artes e criações, planilhas, estratégias, documentos, textos ou outros produtos criados, adquiridos ou manipulados dentro das atividades profissionais dos Colaboradores da Empresa são de propriedade da Empresa e não podem ser copiadas, utilizadas para fins particulares ou enviadas para terceiros.

3. Criação, manipulação, uso e descarte

Toda informação ou ativo desenvolvido em ambiente corporativo deve ser utilizado para propósito do negócio, com uso correto e responsável.

A impressão de documentos contendo informações sensíveis deve ser evitada, mas se houver necessidade para atendimento das demandas profissionais, os documentos devem ser manipulados com acesso restrito.

Os documentos físicos e mídias eletrônicas devem ser descartados de forma segura, evitando a recuperação das informações durante o seu descarte, por exemplo, fragmentar papel e inutilizar mídias digitais fisicamente ou digitalmente com ferramentas apropriadas. Este procedimento inclui dispositivos de armazenamento (*hard disk*) de computadores em desativação.

4. Classificação da informação

Toda informação criada e desenvolvida em ambiente corporativo deve ser classificada apropriadamente de acordo com sua confidencialidade, cabendo ao Gestor da área notificar e orientar seus colaboradores de suas responsabilidades.

5. Conscientização, sensibilização e treinamento de segurança

A área de Segurança da Informação deve estabelecer processos apropriados para disseminação da cultura de Segurança da Informação e Cibernética aos Usuários dos sistemas da Empresa.

Os treinamentos e comunicação podem ser feitos de maneira presencial ou através de ferramentas de comunicação, como plataformas de treinamento online e portais.

Todo novo Usuário deverá ser treinado com conceitos básicos de segurança de informação e, somente após o treinamento, será elegível aos acessos aos sistemas da empresa.

6. Política de continuidade de negócios

A Política de continuidade de negócios visa eliminar ou minimizar os impactos no negócio de falhas de recursos humanos ou de componentes tecnológicos.

Ela é composta pelos seguintes itens:

- Análise de Impacto nos Negócios
- Plano de Continuidade de Negócios
- Plano de Recuperação de Desastre

7. Resposta a incidentes de segurança da informação

Incidentes de segurança da informação são situações em que um ou mais ativos da informação da Empresa estão em risco, ou seja, algum evento confirmado ou sob suspeita relacionado a segurança dos sistemas, serviços ou componentes que suportam os ativos de informação da Empresa.

O plano de resposta a incidentes de segurança da informação tem como objetivo eliminar ou minimizar o impacto do evento no menor tempo possível. Para isso os incidentes devem ser classificados por severidade e as várias áreas participantes devem ter seus papéis definidos para atuação na resolução, comunicação e registro do incidente.

8. Controle de acesso

O controle de acesso tem como objetivo limitar o acesso a sistemas, serviços, informações e recursos somente àqueles necessários para execução das atividades profissionais de cada Usuário.

9. Utilização e aquisição de sistemas e softwares

Todos os sistemas, serviços e softwares utilizados pelo colaborador deverão ser aprovados e homologados pela Empresa.

10. Criptografia de dados

A criptografia é um processo de transformação de dados de forma que eles não tenham mais o formato original e, desta forma, não possam ser lidos sem que se tenha acesso

uma chave de descriptografia. Pode ser implementada através de diversos algoritmos, por sistemas, software ou hardware.

11. Recursos de Tecnologia da Informação

A utilização de algumas disciplinas de tecnologia da informação afeta o nível de segurança do ambiente. Para estas, estão abaixo descritos os requisitos mínimos para sua operação.

11.1 Gestão de ativos

É desejável ter o inventário de ativos de todos os sistemas e serviços da Empresa através de software(s) apropriado para este fim.

11.2 Segurança de redes

Para segurança de redes devem ser implementadas ferramentas de *firewall* para controlar fluxos de dados nas redes internas, externas e internet.

11.3 Operação de recursos computacionais

Os recursos computacionais (servidores, serviços corporativos e dispositivos de rede) devem ser operados por equipe especializada.

11.4 Gestão de estações de trabalho

As estações de trabalho dos Usuários da Empresa devem ser administradas por equipe especializada, seguindo as melhores práticas de mercado para esta prática.

- Devem possuir software de antivírus instalado e ativo.
- Devem ser atualizadas periodicamente com atualizações de segurança, conforme orientação dos fornecedores.

11.5 Monitoração

A monitoração de diversos itens de configuração da infraestrutura da Empresa deve ser periodicamente analisada e, caso haja algum incidente, deve ser registrado e tratado conforme a Política de Gerenciamento de Incidentes.

11.6 Cópias de segurança ou *backup*

Devem ser armazenados cópias de segurança das informações armazenadas em bancos de dados, servidores e outros serviços para recuperação em caso de incidentes.

12. Contratação de serviços de computação em nuvem

Quando houver necessidade de contratação de serviços em nuvem, as áreas de Tecnologia e Segurança de Informação devem ser envolvidas para avaliação de

aderência aos requisitos abaixo, de acordo com a criticidade das informações processadas ou armazenadas:

13. Testes de segurança

Alguns testes de segurança são necessários para avaliar se o nível de segurança dos componentes humanos e tecnológicos estão em níveis adequados.

14. Validade

25/05/2020.

15. Responsáveis

Elaboração	Aprovação
Edson Takayassu Segurança da Informação	Bazili Swioklo CTO -CHIEF TECHNOLOGY OFFICER

16. Histórico

Versão	Data de publicação	Itens alterados	Razões da alteração
01	25/05/2020	-	Reestruturação da Política para contemplar necessidades da Guide Investimentos.