APEX
CAPITAL LTDA

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

1.1 Disposições Gerais

Os sistemas de informação, a infraestrutura tecnológica, os arquivos de dados e as informações internas ou externas, são considerados importantes ativos da empresa, em função da **Apex** apresentar suas operações, dependentes em grande parte da tecnologia para conduzir seus negócios e atender às suas necessidades comerciais e estratégicas.

É necessário que as informações sejam armazenadas, conduzidas e processadas em ambiente seguro e também que todos os usuários da informação compartilhem da responsabilidade pelos processos de segurança definidos neste normativo, com a finalidade de se equiparar às boas práticas das organizações globais.

As normas de segurança da informação estabelecem objetivos, funções, ações, mecanismos de delegação e responsabilidades pelos processos, manipulação da informação e controles internos.

Os processos de segurança da informação devem assegurar a integridade, a disponibilidade e a confidencialidade dos ativos de informação da **Apex**.

- As normas de segurança da informação devem:
  - Proteger os ativos da Apex contra ameaças, internas ou externas, intencionais ou acidentais;
  - Limitar a um nível aceitável a exposição a perdas ou danos que possam resultar em falhas de segurança;
  - Minimizar as ameaças potenciais à segurança das informações, garantindo a manutenção da integridade, disponibilidade e confidencialidade;
  - Assegurar que os recursos adequados estarão disponíveis para implementar e manter um programa de segurança efetivo;
  - Conscientizar os associados e usuários da informação, sobre aspectos relacionados à segurança das informações.

1.2 Uso da Informação

- Aplicam-se as seguintes atribuições aos usuários da informação:
- O proprietário é responsável pela geração, exatidão e classificação das informações;
- O gestor é responsável pela gerência das informações e pela definição dos direitos de acesso às mesmas;
- O custodiante é responsável pela guarda e disponibilidade das informações;
- O usuário é responsável pelo uso adequado das informações e seus ativos a que tenha acesso.

1.3 Responsabilidades

- Da Diretoria:
  - Direcionar os esforços e recursos propostos para a segurança da informação, de acordo com a estratégia de negócios da empresa;
  - Aprovar as normas de segurança da informação e suas atualizações;
  - Aprovar os controles a serem utilizados para garantir a segurança das informações;
  - Acompanhar os indicadores de segurança e os incidentes reportados pela empresa prestadora de serviços de TI;
  - Comunicar à área de Compliance os casos de violações à Norma de Segurança da Informação para as providências necessárias;
  - Apoiar as iniciativas para melhoria contínua de medidas de proteção da informação da empresa, com vistas a reduzir os riscos identificados;
  - Aprovar o planejamento, alocação de verbas, os recursos humanos e de tecnologia, no que tange a segurança da informação;
  - Delegar as funções de segurança da informação aos profissionais responsáveis.

- Da Empresa Prestadora de Serviços de TI:
  - Monitorar as violações de segurança e tomar ações corretivas visando saná-las e cuidando para que não haja recorrência;
  - Orientar os testes da infraestrutura de tecnologia e de sistemas para avaliar os pontos fracos e detectar possíveis ameaças;
  - Assessorar as demais áreas da empresa no processo de classificação das informações;
  - Auxiliar as áreas de negócio na elaboração do Plano de Continuidade dos Negócios específico de cada uma;

- Assegurar que exista um processo apropriado para a comunicação dos incidentes e violações de segurança detectados pelos usuários da informação, independentemente dos recursos tecnológicos utilizados;
- Identificar recursos e fornecer orientação para a tomada de ações rápidas caso sejam detectados incidentes de segurança;
- Manter a infraestrutura que suporta o ambiente controlado;
- Manter a infraestrutura e sistemas atualizados;
- Garantir a implementação e operação dos indicadores de segurança;
- Notificar imediatamente os incidentes de segurança à diretoria;
- Garantir a rápida tomada de ações em caso de incidentes de segurança.

♦ Da área de *Compliance* (ou responsável por estas funções):

- Gerenciar os problemas disciplinares resultantes de violações dos controles de segurança da informação, juntamente com os gestores dos envolvidos;
- Emitir o Termo de Responsabilidade e Compromisso de Sigilo sobre Segurnça da Informação e garantir a ciência deste entre todos os colaboradores. No final deste documento encontra-se um modelo de Termo de Responsabilidade (Anexo A);
- Gerenciar a assinatura do Acordo de Confidencialidade quando da contratação de terceiros ou prestadores de serviços. No final deste documento encontra-se um modelo de Acordo de Confidencialidade;
- Determinar as sanções cabíveis de acordo com a legislação em vigor.

♦ Dos Auditores Independentes:

- Garantir, mediante verificações de conformidade, que a Apex esteja operando de acordo com os princípios e controles estabelecidos na Norma de Segurança da Informação;
- Emitir pareceres para a Diretoria e para os clientes da Apex;
- Revisar periodicamente a Norma de Segurança da Informação e sugerir as alterações necessárias.
-

1.4 Itens Abordados pela Segurança da Informação

Controle e Classificação dos Ativos

Este tópico visa assegurar que todos os ativos, físicos ou lógicos, estejam identificados, classificados e que sejam controlados.

- Todos os ativos da Apex, sejam estes físicos ou lógicos, devem ser adequadamente controlados pelo departamento de contabilidade. Os ativos devem ser protegidos de acordo com o grau de criticidade que representam para o negócio da Apex;
- É necessário que todos os ativos sejam classificados de acordo com os critérios definidos pela Diretoria da Apex;
    - Com base nessa classificação, devem ser adotados controles que garantam as três propriedades básicas desses ativos: integridade, disponibilidade e confidencialidade, em um nível proporcional à criticidade que representam para o negócio da Apex.
- Em caso de dúvida, nenhuma informação deve ser divulgada.

Segurança de Pessoal

Neste caso, a norma visa assegurar que todos os usuários da informação tenham conhecimento dos requisitos e das obrigações definidos pela Norma de Segurança da Informação, assim como minimizar a ocorrência de incidentes de segurança em função de problemas no uso, desvio de informações, fraudes e na interpretação das normas e procedimentos, e de falhas no processo de conscientização sobre segurança.

- Todos os usuários da informação e clientes devem conhecer e adotar as definições de segurança da informação instituídas pela Apex e suas responsabilidades na manutenção da segurança corporativa;
- Os usuários da informação devem ser orientados sobre os procedimentos e o uso correto dos recursos de processamento das informações, de forma a minimizar possíveis riscos de segurança.

Segurança Física

Em termos de segurança física, a norma deve definir os requisitos mínimos de segurança física que os ambientes considerados críticos, onde há informações sigilosas da **Apex**, devem possuir para assegurar a proteção de seus ativos contra fatores que possam causar interrupção das atividades, alteração ou vazamento das informações e consequente prejuízo financeiro.

- Todas as áreas classificadas como críticas na Apex devem estar protegidas por controles físicos apropriados;
    - Esses controles devem ser proporcionais à criticidade dos equipamentos, dos sistemas e das informações mantidas e manuseadas nestas áreas.
- As áreas classificadas como críticas devem estar devidamente protegidas por acesso não autorizado, dano ou interferência.

Controle de Acesso às informações

O controle de acesso às informações deve definir os requisitos necessários para que o usuário da informação obtenha acesso ao ambiente de tecnologia da **Apex**.

- O acesso a todos os sistemas e informações da Apex deve ser concedido de acordo com as necessidades da função do usuário para a execução de suas atividades;
- O responsável pelos sistemas ou da informação é o responsável pela concessão de acesso a todos os recursos que estejam sob sua responsabilidade. Os acessos concedidos deverão ser periodicamente revisados;
- Os usuários devem se restringir às informações e ambientes aos quais estão autorizados, devendo acessá-los somente se houver a necessidade para desempenho de suas atividades profissionais.

Desenvolvimento e Manutenção de Sistemas

Este item enumera os requisitos de segurança para desenvolvimento, manutenção e parametrização de sistemas.

- Todos os sistemas desenvolvidos pela Apex ou por empresas contratadas por esta, deverão atender aos requisitos de segurança definidos pela Norma de Segurança da Informação.

Gerenciamento da Continuidade dos Negócios

A Norma de Gerenciamento da Continuidade dos Negócios deve identificar atividades chaves que compõem um Plano de Continuidade de Negócios, a fim de assegurar que as operações da **Apex** sejam rapidamente retomadas em caso de incidentes graves.

- É necessário que exista um Plano de Continuidade de Negócios que assegure a continuidade ou a rápida retomada das atividades em caso de falhas ou interrupções dos negócios;
    - O Plano de Continuidade de Negócios deve incluir os processos, procedimentos e alternativas para recuperação de qualquer interrupção do negócio, independentemente do agente causador, além da proteção dos processos críticos da **Apex** contra efeitos de desastres significativos.

Conformidade

A Norma de Conformidade deve definir as ações necessárias para que a **Apex** não viole nenhuma lei civil ou criminal, estatutos, regulamentações ou obrigações contratuais referentes a quaisquer requisitos de segurança.

- A empresa deve estar em conformidade com todas as regras e regulamentos instituídos por lei. Isto inclui qualquer lei civil ou criminal, estatutos ou obrigações contratuais feitas envolvendo a **Apex**;
- É responsabilidade de todos os usuários de informações auxiliar na manutenção dos requisitos de segurança e nos regulamentos ditados por lei.