Política de Segurança das Informações e Segurança Cibernética

22 de Fevereiro de 2024

I - POLÍTICA DE SEGURANÇA DAS INFORMAÇÕES

I.1 - DEFINIÇÃO

A Política de Segurança das Informações da Smartquant Investimentos Ltda. ("Smartquant") deve proteger as informações como um todo, tanto no ambiente físico, como também no ambiente digital, garantindo a proteção da tecnologia, dos procedimentos e das pessoas naturais.

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

As informações estão presentes sob diversas formas, coforme mencionado a seguir: **(i)** sistemas; **(ii)** diretórios de rede; **(iii)** banco de dados; **(iv)** materiais impressos; **(v)** materiais em arquivos eletrônicos; **(vi)** equipamentos fixos e portáteis; e **(vii)** por meio comunicação oral, principalmente em conversas realizadas em locais públicos.

É necessário que as informações sejam armazenadas, conduzidas e processadas em ambiente seguro e também que todos os usuários das informações compartilhem da responsabilidasde pelos processos de segurança definidos nesta Política, com a finalidade de estar em conformidade às normas regulatórias vigentes.

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

Os processos de segurança das informações devem assegurar a **(i)** confidencialidade, **(ii)** integridade e a **(iii)** disponibilidade dos ativos e das informação da Smartquant.

(i) Confidencialidade: garantir que o acesso às informações seja obtido exclusivamente por pessoas autorizadas.

(ii) Integridade: garantir que as informações seja mantidas íntegras, visando protegê-las sem modificações indevidas, na guarda ou na transmissão, contra eventuais alterações indevidas, propositais ou acidentais.

(iii) Disponibilidade: garantir que as pessoas autorizadas tenham acesso à informação sempre que necessário.

As normas de Segurança das Informações estão divididas da seguinte forma:

(i) proteger os ativos da Smartquant e de seus clientes contra ameaças, internas ou externas, intencionais ou acidentais;

(ii) gerenciar os acessos das pessoas físicas autorizadas;

(iii) limitar a um nível aceitável a exposição a perdas e/ou danos que possam resultar em falhas de segurança;

(iv) minimizar as ameaças potenciais à segurança das informações, garantindo a manutenção da integridade, disponibilidade e confidencialidade;

(v) assegurar a autenticidade, a irretratabilidade e a conformidade; e

(vi) conscientizar os usuários das informações sobre aspectos relacionados à segurança das informações.

I.2 - USO DAS INFORMAÇÕES

Aplicam-se as seguintes atribuições aos usuários das informações:

(i) a Smartquant é responsável pela geração, exatidão e classificação das informações;

(ii) a Smartquant é responsável pela gerência das informações e pela definição dos direitos de acesso às mesmas;

(iii) O custodiante é responsável pela guarda e disponibilidade das informações;

(iv) O usuário é responsável pelo uso adequado das informações e seus ativos a que tenha acesso.

I.3 - RESPONSABILIDADES

I.3.1 - Da Diretoria de *Compliance*:

(i) direcionar os esforços e recursos propostos para a segurança das informações, de acordo com a estratégia da Smartquant;

(ii) aprovar as normas de segurança das informações e suas atualizações;

(iii) aprovar os controles a serem utilizados para garantir a segurança das informações;

(iv) apoiar as iniciativas para melhoria contínua de medidas de proteção da informação da Smartquant, com vistas a reduzir os riscos identificados;

(v) delegar as funções de segurança das informações a profissionais responsáveis; Desenvolver, manter e implementar programas de treinamento e de conscientização aos colaboradores, sobre a Política de Segurança, a forma como ela está estruturada e os principais conceitos de segurança das informações;

(vi) gerenciar os problemas disciplinares resultantes de violações dos controles de segurança das informações; e

(vii) determinar as sanções cabíveis.

I.3.2 - ITENS ABORDADOS PELA SEGURANÇA DAS INFORMAÇÕES

I.3.2.1 - CONTROLE E CLASSIFICAÇÃO DOS ATIVOS

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

Todos os ativos da Smartquant, sejam estes físicos ou tecnológicos, devem ser adequadamente controlados. Os ativos devem ser protegidos de acordo com o grau de criticidade que representam para a Smartquant.

É necessário que todos os ativos sejam classificados de acordo com os critérios definidos pela Diretoria de *Compliance* da Smartquant.

Com base nessa classificação, devem ser adotados controles que garantam as 3 (três) propriedades básicas desses ativos: integridade, disponibilidade e confidencialidade, em um nível proporcional à criticidade que representam para a Smartquant.

Em caso de dúvida, nenhuma informação deve ser divulgada.

I.3.2.2 - CONTROLE DE ACESSO À 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 Smartquant.

O acesso a todos os sistemas e informações da Smartquant 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 o desempenho de suas atividades profissionais.

Todos os Colaboradores devem ter ciência de que o uso das informações e dos sistemas de informação da Smartquant é monitorado, e que os registros assim obtidos poderão ser utilizados para detecção de violações do Manual e, conforme o caso, servir como evidência em processos administrativos e/ou legais.

I.3.2.3 - USO DE EQUIPAMENTOS E SISTEMAS

Cada Colaborador é responsável ainda por manter o controle sobre a segurança das informações armazenadas ou disponibilizadas nos equipamentos que estão sob sua responsabilidade.

A utilização dos ativos e sistemas da Smartquant, incluindo computadores, telefones, internet, e- mail e demais aparelhos se destina prioritariamente a fins profissionais. O uso indiscriminado destes para fins pessoais deve ser evitado e nunca deve ser prioridade em relação a qualquer utilização profissional.

Todo Colaborador deve ser cuidadoso na utilização do seu próprio equipamento e sistemas e zelar pela boa utilização dos demais. Caso algum Colaborador identifique a má conservação, uso indevido ou inadequado de qualquer ativo ou sistemas deve comunicar o fato a qualquer dos membros do Comitê de Compliance e Risco.

I.3.2.4 - ACESSO REMOTO

A Smartquant permite o acesso remoto pelos Colaboradores, de acordo com a prévia autorização do Diretor de Compliance e Risco.

Ademais, os Colaboradores autorizados serão instruídos a:

(i) manter softwares de proteção contra malware/antivírus nos dispositivos remotos;

(ii) relatar ao Diretor de Compliance e Risco qualquer violação ou ameaça de segurança cibernética ou outro incidente que possa afetar informações da Smartquant e que ocorram durante o trabalho remoto; e

(iii) não armazenar Informações Confidenciais ou sensíveis em dispositivos pessoais.

II - POLÍTICA DE SEGURANÇA CIBERNÉTICA

II.1 - DEFINIÇÕES

A segurança cibernética é o conjunto de tecnologias, processos e práticas projetados para proteger a rede, os computadores, os sistemas e os dados de ataques ou acessos não autorizados.

O risco de ataque cibernético ameaça os princípios da segurança das informações, tais como confidencialidade, integridade e disponibilidade.

Há diversas razões para que esses ataques ocorram e os principais motivos são:

(i) obter recursos financeiros;

(ii) roubar e manipular informações;

(iii) obter informações privilegiadas;

(iv) sabotagem à instituição;

(v) disseminar falsas notícias; e

(vi) disseminar o caos.

A segurança cibernética deve garantir:

(i) a segurança dos sistemas e dos bancos de dados;

(ii) o gerenciamento das pessoas autorizadas;

(iii) a segurança dos sistemas e informações que estão na nuvem;

(iv) a segurança para todos os dispositivos/equipamentos;

(v) o planejamento da continuidade do negócio; e

(vi) o treinamento constante do usuário final, com o objetivo de minimizar a vulnerabilidade da organização.

São exemplos de consequencias/danos que podem ser causados pela falha na segurança cibernética:

(i) risco de imagem;

(ii) risco de continuidade do negócio; e

(iii) prejuízos financeiros.

II.2 - IDENTIFICAÇÃO DOS RISCOS

A empresa prestadora de serviços de TI é a responsável pelo mapeamento dos riscos internos e externos, dos equipamentos e s*oftwares* utilizados pela Smartquant.

A Diretoria de *Compliance* da Smartquant é responsável pela análise dos riscos mapeados e pela implantação/investimento dos processos que precisam de proteção e monitamento.

II.3 - AÇÕES DE PREVENÇÃO E PROTEÇÃO

Todo o procedimento operacional é monitorado por empresa prestadora de serviços de TI, especializada em TI.

II.4 - MONITORAMENTO E TESTES

A empresa prestadora de serviços de TI é a responsável pelo monitoramento e emite relatórios semanais e mensais que medem a disponibilidade dos servidores e das estações de trabalho contendo a relação das atualizações realizadas e possíveis pontos de vulnerabilidades, serviços do *windows* e atualizações dos antivírus.

II.5 - PLANO DE RESPOSTAS

A capacidade e efetividade do plano de resposta é vital para proteger as informações e os recursos de informação da Smartquant, clientes e usuários.

Todo o procedimento operacional é monitorado. Os recursos de TI são monitorados por sistemas automatizados que fornecem informações atualizadas sobre a indisponibilidade dos serviços com registro de incidentes para providências e encaminhamento de soluções e está preparada para possibilitar um plano de resposta de forma ágil e consistente.

Caso a Smartquant sofra algum ataque cibernético que ocasione a perda de acesso aos sistemas, os responsáveis por cada área estão autorizados a acionar a equipe de *help desk* da empresa prestadora de serviços de TI e ativar os acessos aos sistemas de *back-up* em nuvem da Smartquant, de forma que todo o trabalho operacional possa ser mantido.

III - REVISÃO

Esta Política de Segurança das Informações e de Segurança Cibernnética será revisada, no mínimo, anualmente pela Diretoria de *Compliance*. Serão utilizadas como base para a sua atualização as legislações, instruções, e regulamentações e autorregulamentações vigentes na data da sua revisão e estará vigente e aplicável mesmo durante o período de licenças/ausências dos membros na Smartquant.

IV - SANÇÕES

Esta Política de Segurança das Informações e de Segurança Cibernnética se aplica a todos os usuários da rede corporativa da Smartquant, a quem caberá o atendimento às diretrizes e procedimentos ora estabelecidose, de forma a informar à Diretoria de *Compliance* sempre que se presenciar o seu descumprimento.

São exemplos que podem ocasionar em sanções:

(i) uso ilegal de *software*;

(ii) introdução intencional de vírus;

(iii) acesso a dados e sistemas não autorizados; e

(iv) divulgação de informações confidenciais.

Os colaboradores que violarem essa Política estarão sujeitos aos cumprimentos de determinadas sanções, tais como:

(i) responsabilidade civil por perdas e danos provocados aos fundos e/ou clientes da Smartquant;

(ii) ação disciplinar por parte dos agentes reguladores e autorreguladores, incluindo a revogação de autorização e multas;

(iii) responsabilidade criminal; e

(iv) advertência verbal, advertência escrita ou rescisão contratual, conforme a gravidade do caso.

V. DISTRIBUIÇÃO DA POLÍTICA

Esta política será distribuída eletronicamente para todos os usuários da Smartquant.

Existirá uma versão impressa dessa política, que estará organizada em uma pasta de documentação e que ficará disponível para consulta dos envolvidos, nos arquivos da Smartquant.

Quando ocorrerem revisões ou atualizações na política, todos os envolvidos e os aprovadores receberão uma nova versão eletrônica. Uma nova versão impressa substituirá a versão anterior existente na Smartquant e todas as versões anteriores deverão ser descartadas.