1. Objetivo

Estabelecer as diretrizes e nortear procedimentos referentes à segurança da informação e cibernética de forma a proporcionar disponibilidade, integridade e confidencialidade, bem como prevenir, detectar e reduzir a vulnerabilidade a incidentes no que tange ao ambiente cibernético, aos dados e sistemas de informação utilizados.

2. Abrangência

Política aplicável a todos os membros da diretoria, gerentes e demais colaboradores, fornecedores e prestadores de serviços da QS Intelligence Comércio e Serviço LTDA (QSI)

3. Responsabilidades

Diretoria e gerentes:

Assegurar o comprometimento de todos os administradores, colaboradores, fornecedores e terceiros, com atuação ética e responsável quando da ocorrência e comunicação de incidentes;

Compartilhar informações com os responsáveis pelo seu tratamento em tempo hábil, tomando todas as ações cabíveis para minimizar os potenciais danos;

Ser responsável pelo cumprimento desta Política e pela melhoria contínua dos procedimentos relacionados com a segurança da informação e cibernética.

Assegurar a implantação, acompanhar e monitorar o cumprimento das diretrizes desta Política, revisá-la anualmente e mantê-la atualizada;

Chief Informativo Security Officer (CISO)

O Chief Information Security Officer (CISO) é responsável por liderar e gerenciar a segurança da informação da organização. Suas principais responsabilidades incluem:

Relatório regular sobre o status da segurança, ameaças e incidentes relevantes.

Condução de programas de conscientização e treinamento em segurança para os colaboradores.

Coordenação da resposta a incidentes de segurança, incluindo análise, contenção e mitigação de impactos.

Garantia da conformidade com regulamentações, leis e normas aplicáveis, como LGPD e GDPR.

Gestão de riscos relacionados à segurança da informação e cibersegurança.

Definição e supervisão das políticas, procedimentos e controles de segurança da informação.

Desenvolvimento e implementação da estratégia de segurança da informação alinhada aos objetivos de negócios.

Colaboradores, Fornecedores e Terceiros:

Atuar de forma ética e responsável pela proteção e salvaguarda dos ativos e informações de que sejam usuários ou com os quais tenham contato, como de seus clientes, parceiros e fornecedores, dos ambientes físicos e computacionais a que tenham acesso, independentemente das medidas de segurança implantadas e em cumprimento a esta Política.

4. Diretrizes

A QSI, para garantir a segurança da informação e cibernética, exerce suas atividades com base nos seguintes pilares:

Disponibilidade: garantir que a informação estará disponível sempre que for necessário.

Integridade: garantir que a informação, armazenada ou em trânsito, não sofrerá qualquer modificação não autorizada, seja esta intencional ou não.

Confidencialidade: garantir que a informação somente estará acessível para pessoas autorizadas.

Independentemente da forma apresentada, compartilhada ou armazenada, dados devem ser utilizados apenas para as suas respectivas finalidades, sendo sujeitos a monitoramento.

Requisitos de segurança da informação são estabelecidos levando-se em consideração a avaliação dos riscos que possam afetar negativamente a estratégia e os objetivos gerais de negócios da Companhia, o cumprimento de exigências legais, regulamentares e contratuais e proteção das informações em todo o seu ciclo de vida, em meios físicos ou digitais.

Na gestão da informação a integridade, a confidencialidade e a disponibilidade são asseguradas durante todas as fases de tratamento.

Informações relacionadas a ameaças à segurança da informação e cibernética devem ser coletadas e analisadas para apoiar o aprimoramento dos recursos de proteção.

No gerenciamento de identidades, os privilégios de acesso devem estar associados a cada pessoa.

A segurança da informação é aplicada em todas as fases do ciclo de vida dos sistemas e outros ativos de informação.

Na contratação de serviços ou de pessoas e no relacionamento com colaboradores, parceiros, intermediários, contratados e estagiários são observados os mesmos quesitos de segurança..

Nos casos de violação ou divulgação indevida de informações, a ocorrência é analisada sob o aspecto legal e disciplinar, imputando responsabilização, e sob o aspecto técnico, corrigindo as vulnerabilidades.

Com relação às diretrizes de segurança da informação e cibernética, a QSI se compromete a:

Resguardar a proteção dos dados contra acessos indevidos, bem como contra modificações, destruições ou divulgações não autorizadas.

Classificar os dados e informações quanto à relevância para o negócio, garantindo a continuidade dos negócios, a partir de diretrizes emanadas por essa Política.

Efetuar regularmente procedimentos para identificar, analisar, avaliar e tratar os riscos por uso indevido da informação, fraudes ou atos que possam danificar ou impedir o acesso aos dados e sistemas de informação.

Sensibilizar, conscientizar, capacitar e avaliar, periodicamente, os colaboradores sobre os aspectos relacionados ao adequado desempenho das suas atividades dentro das diretrizes de segurança da informação e cibernética, de forma a disseminar a cultura de segurança da informação e cibernética, inclusive quanto a prestação de informações a usuários finais sobre precauções na utilização de produtos e serviços oferecidos, quando aplicável.

Adotar procedimentos e controles para reduzir a vulnerabilidade da Companhia a incidentes e atender aos objetivos de segurança cibernética com relação às medidas de segurança, dentre eles:

- A autenticação;
- A criptografia;
- A prevenção e a detecção de intrusão;
- A prevenção de vazamento de informações;
- A realização periódica de testes e varreduras para detecção de vulnerabilidades;
- A proteção contra softwares maliciosos;
- Os controles de acesso e de segmentação da rede de computadores;
- E a manutenção de cópias de segurança dos dados e das informações.

Aplicar procedimentos e controles, inclusive, no desenvolvimento de sistemas de informação seguros e na adoção de novas tecnologias empregadas nas atividades da Companhia.

Conceder a terceiros somente o acesso às informações necessárias ao exercício de suas atividades, desde que tal acesso não implique o descumprimento de legislação ou regulamentação em vigor, observando-se, ainda, o contido na cláusula contratual de confidencialidade do uso.

Aplicar proteção aos serviços de processamento e armazenamento de dados em nuvem, servidores, sistemas operacionais e demais componentes que compõem o ambiente de infraestrutura, para garantia da segurança da informação e cibernética.

Permitir a terceirização de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem, no País ou no exterior, seguindo critérios específicos de decisão para matéria desta natureza.

Assegurar que a engenharia dos sistemas de informação em uso, desenvolvidos ou mantidos pela Companhia, os fornecidos por terceiros ou outras tecnologias adotadas concorram para o cumprimento das demais diretrizes desta Política.

Assegurar que um plano de ação e de resposta a incidentes esteja estabelecido visando à implementação desta política.

Assegurar a completa gestão do ciclo de tratamento de incidentes relevantes à segurança da informação no negócio,

Adotar iniciativas para compartilhamento de informações sobre os incidentes relevantes por meio de filiação em fóruns de discussão.

Adotar os procedimentos que garantam a recuperação dos dados e sistemas de informação corporativos para a continuidade dos negócios, os quais devem contemplar a execução periódica de testes, a partir de cenários de incidentes relevantes e de substituição da empresa contratada.

Garantir o cumprimento dos períodos de retenção e expurgo de informações relacionadas à gestão da segurança da informação e cibernética.

Assegurar a implementação dos controles específicos voltados para a rastreabilidade no tratamento de informações sensíveis para o negócio.

Assegurar que esta política seja divulgada aos colaboradores e empresas prestadoras de serviços a terceiros da Companhia, além de mantê-la num local de fácil acesso a todos os envolvidos.

5 Disposições Gerais

Esta Política entra em vigor na data de sua aprovação pela diretoria e revoga quaisquer documentos em contrário.

Comunicamos que os colaboradores, fornecedores ou outros stakeholders que observarem quaisquer desvios às diretrizes desta Política, poderão entrar em contato através do e-mail ou telefone no site www.qsintelligence.com.br, podendo ou não se identificar.

Internamente, a não observância das determinações desta Política acarretará ações de gestão de consequência que poderão variar desde uma orientação sobre como proceder para anular ou, ao menos, minimizar os eventuais problemas criados, até a demissão por justa causa dos responsáveis.

Para os casos externos, o descumprimento das diretrizes desta Política enseja a aplicação de medidas cíveis e/ou criminais, conforme a respectiva gravidade do seu descumprimento.

Recife, 11 de Dezembro de 2024.

QS INTELLIGENCE COMÉRCIO E SERVIÇO LTDA.

Rodrigo Freire de Menezes