ICON CAPITAL
Gestão de Investimentos

Política de Segurança da Informação e Segurança Cibernética

Elaboração	Versão
03/2024	1.0
03/2025	1.1
01/2026	1.2

Índice

INTRODUÇÃO

A Política de Segurança da Informação e Segurança Cibernética da Icon Capital é um documento fundamental que define as diretrizes corporativas para proteger os dados e informações da empresa. Ela visa garantir a segurança e o sigilo de informações confidenciais, além de prevenir e mitigar riscos e responsabilidades legais para todos os seus usuários.

A política deve ser seguida e implementada em todas as áreas da empresa, abrangendo não apenas os funcionários diretamente ligados à empresa, como sócios, diretores e administradores, mas também terceiros contratados que tenham acesso às informações da empresa.

O principal objetivo da Segurança da Informação é garantir a confidencialidade, integridade e disponibilidade das informações utilizadas pela Icon Capital em suas operações. Isso significa que as informações devem ser protegidas contra acessos não autorizados (confidencialidade), garantindo que não sejam alteradas indevidamente (integridade) e que estejam acessíveis quando necessário (disponibilidade).

Para alcançar esses objetivos, a política define práticas e procedimentos adequados para manipular, controlar, proteger e, quando necessário, descartar as informações de forma segura, garantindo que os dados sensíveis da empresa sejam tratados com o devido cuidado e segurança.

1. PROPÓSITO

A Política de Segurança da Informação da Icon Capital é um documento fundamental para garantir a segurança dos dados da empresa e dos indivíduos. Ela define os princípios e diretrizes que norteiam o comportamento dos colaboradores em relação à segurança da informação.

A implementação da política é essencial para proteger os interesses da empresa e dos indivíduos, além de garantir o cumprimento das leis de proteção de dados. A seguir são apresentados os principais aspectos que são levados em conta nesta Política:

Aspecto	Descrição
Confidencialidade	Assegurar que somente indivíduos autorizados tenham acesso a informações específicas, fontes ou sistemas.
Integridade	Garantir que as informações permaneçam em seu estado original, protegendo-as contra alterações indevidas, intencionais ou acidentais, durante armazenamento e transmissão.
Disponibilidade	Garantir que os dados estejam acessíveis sempre que necessário para usuários autorizados, assegurando um acesso seguro, rápido e eficiente.

Autenticidade	Garantir a verificação da identidade dos usuários e que as informações provenham da origem anunciada, evitando qualquer forma de falsificação ou manipulação.
Auditoria	Assegurar o cumprimento da política geral de segurança da informação através de processos de auditoria regulares.

Essa política visa estabelecer um ambiente seguro para as informações da Icon Capital, protegendo não apenas os interesses da empresa, mas também os dados sensíveis dos indivíduos envolvidos.

2. IMPLEMENTAÇÃO DA POLÍTICA

Este documento estabelece os princípios e orientações para salvaguardar as informações da Icon Capital, abrangendo todos os colaboradores, prestadores de serviços e outras partes envolvidas no manejo das informações da empresa, independentemente do formato ou meio.

Desde que haja aviso prévio, os espaços, sistemas, dispositivos eletrônicos e conexões da empresa estão sujeitos a monitoramento e registro, conforme as leis nacionais.

O uso de aplicativos de mensagens em dispositivos pessoais para assuntos profissionais deve seguir os mesmos protocolos de segurança da informação estabelecidos pela política, considerando a relação de confiança entre as partes envolvidas.

Cada colaborador tem o dever de manter-se atualizado com relação a esta política, assim como aos procedimentos e regulamentos pertinentes. Isso inclui o uso adequado de arquivos e informações eletrônicas, preservando a segurança dos recursos computacionais sob sua responsabilidade e mantendo a integridade e confidencialidade dos dados nos dispositivos.

Em situações de dúvida relacionadas à obtenção, utilização ou descarte de informações, os colaboradores devem procurar orientação junto ao Diretor de Compliance.

A Diretoria de Compliance é encarregada de fornecer treinamento a todos os funcionários e de monitorar de forma especial aqueles que têm acesso a informações confidenciais, reservadas ou privilegiadas, e participam do processo de tomada de decisão de investimento.

O Departamento de Compliance tem o papel de supervisionar, apoiar e estabelecer controles para garantir a confiabilidade e a rastreabilidade das informações comerciais da empresa, incluindo o controle de acesso aos sistemas e registros, aplicação de procedimentos internos para lidar com vazamentos de informações e realização de testes periódicos nos sistemas e procedimentos conforme estabelecidos na Política de Controles Internos.

A Área de Tecnologia da Informação (TI) na Icon Capital é encarregada de diversas responsabilidades fundamentais, como garantir a integridade, disponibilidade e confidencialidade dos sistemas, arquivos, informações e ativos tecnológicos da empresa, além de controlar eficazmente as permissões de acesso concedidas a colaboradores e terceiros e manter as soluções de segurança operacionais e em conformidade com os procedimentos internos.

Outro aspecto crucial é assegurar que as soluções de segurança, como criptografia, backup, antivírus e AntiSpam, estejam operacionais e em conformidade com os procedimentos internos estabelecidos. Isso envolve a implementação e manutenção de ferramentas e protocolos de segurança atualizados para proteger os sistemas e dados da empresa contra ameaças cibernéticas.

Além disso, a área de TI também é responsável por controlar o acesso à internet de acordo com as regras internas de uso, garantindo que os recursos online sejam utilizados de maneira segura e em conformidade com as políticas da empresa.

A contínua adesão e atualização em relação a essas diretrizes são essenciais para assegurar um ambiente de trabalho seguro e protegido contra possíveis ameaças cibernéticas e riscos de segurança da informação.

3. ACESSO AOS SISTEMAS/RECURSOS DE REDE

Cada funcionário é encarregado da posse e utilização adequada de seus próprios logins, senhas e autorizações de acesso, sendo estritamente proibido o compartilhamento dessas informações em qualquer situação.

O acesso aos sistemas de informação é concedido apenas a indivíduos autorizados e limitado ao necessário para desempenhar suas respectivas funções. Qualquer acesso considerado desnecessário ou com privilégios excessivos será revogado, enquanto o acesso remoto é permitido apenas mediante a segurança adequada dos dispositivos.

A concessão de acesso aos sistemas da Icon Capital é realizada mediante autorização do proprietário correspondente, seguindo o princípio do acesso mínimo necessário. A empresa efetua monitoramento contínuo dos recursos de rede e sistemas, incluindo registros de auditoria em diversos meios, como telefonia, computadores, e-mails e acesso à internet, mantendo a privacidade dos colaboradores enquanto utiliza tais informações para investigações internas ou para cumprir medidas judiciais.

Todos os acessos e tentativas de acesso são devidamente registrados nos sistemas da empresa, incluindo o monitoramento dos ramais de telefonia a fim de identificar possíveis usos inadequados.

4. DISPOSIÇÕES FINAIS

Em caso de vazamento de informações confidenciais, o Diretor de Risco e Compliance irá discutir com a Diretoria, e se necessário, com o Responsável pela Segurança Cibernética, o melhor plano efetivo de recuperação e as medidas para minimizar e prevenir danos.

Os colaboradores da Icon Capital são obrigados a reportar à área de Compliance qualquer violação das normas de segurança da informação que presenciarem. Todas as violações ou desvios serão investigados para determinar as medidas necessárias, visando corrigir falhas ou reestruturar processos.

A revisão dos parâmetros e premissas deste documento, bem como de outros manuais e políticas, deve ocorrer anualmente ou quando solicitado, sendo de responsabilidade do Diretor de Compliance.

Todos os documentos utilizados ou gerados para a manutenção da política de segurança da informação, seja em meio eletrônico ou físico, devem ser arquivados pelo período mínimo de 5 (cinco) anos, em conformidade com as recomendações dos órgãos regulatórios e com as políticas internas da Icon Capital.