POLÍTICA DE SEGURANÇA CIBERNÉTICA

Versão 2.0
Revisado em: 03/06/2023

Atividade	Área
Elaboração	Área de *Compliance*
Revisão	Diretor de *Compliance* e Riscos
Aprovação	Diretor de *Compliance* e Riscos

Classificação das Informações
[ ] Uso Interno [X] Uso Público

1. Objetivo

Estabelecer as regras e diretrizes pertinentes à Segurança Cibernética e instituí-las junto aos processos que possuem acesso as informações sensíveis de clientes e parceiros do Grupo Actum Capital, em conformidade com o determinado pela Diretoria, pelas normas e legislação vigentes.

A segurança da informação está entre um dos tópicos mais relevantes dentro de uma organização. As informações fazem parte do patrimônio da empresa e estão sob constante risco. A sua perda ou roubo representa um prejuízo significativo para a estratégia do negócio.

Dessa forma, a confidencialidade, integridade e disponibilidade da informação são pilares diretamente ligados ao tema de Segurança.

Com o objetivo de minimizar esses riscos, a Política tem como finalidade estabelecer princípios e diretrizes de proteção de dados pessoais e informações sigilosas contra ameaças cibernéticas em complemento à Política de Segurança da Informação do Grupo Actum Capital.

2. Aplicação

Esta política se aplica à Actum Capital Gestão de Recursos Ltda. (“Actum Capital”), administradora de carteiras de títulos e valores mobiliários (Gestora) do Grupo Actum Capital, nos termos da resolução CVM nº 21, de 25 de fevereiro de 2021 e demais empresas do grupo

3. Definições

Riscos Cibernéticos: são os riscos de ataques cibernéticos, oriundos de malware, técnicas de engenharia social, invasões, ataques de rede (DDoS e Botnets), fraudes externas, entre outros, que possam expor Dados, redes e sistemas do Grupo Actum Capital, causando danos financeiros e/ou de reputação consideráveis, podendo, em algumas circunstâncias, prejudicar a continuidade das atividades do Grupo Actum Capital e empresas controladas.

Serviços Relevantes: Serviços prestados por Prestadores de Serviço às empresas do Grupo Actum Capital cuja indisponibilidade, vulnerabilidade ou inconsistência possa prejudicar a continuidade de seus negócios: (i) afetando o atendimento ofertado ao Cliente; (ii) paralisando a operação do Grupo Actum Capital, podendo causar perdas financeiras; ou (iii) impedindo o fornecimento de informações pelas empresas do Grupo Actum Capital aos entes reguladores e/ou o cumprimento de direitos e garantias dos clientes.

Incidentes: Qualquer ocorrência que realmente ou potencialmente comprometa a confidencialidade, integridade ou disponibilidade de um sistema de informação ou a informação que o sistema processa, armazena ou transmite ou que constitui uma violação ou ameaça iminente de violação de políticas de segurança, procedimentos de segurança ou políticas de uso aceitáveis. São considerados incidentes, mas não se limitando a esses:

(i) acesso indevido a contas e/ou sistemas do Grupo Actum Capital;
(ii) acessos não autorizados a bases de Dados ou Informações de uso interno ou confidencial do Grupo Actum Capital;
(iii) alteração ou perda de Dados ou Informações, ou de acesso a sistemas ou ambientes lógicos, bem como da integridade destes;
(iv) vulnerabilidades existentes nos sistemas, bem como situações de indisponibilidade dos sistemas e/ou das informações ou
(v) demais falhas de segurança que acarretem acessos não autorizados a sistemas ou ambientes tecnológicos do Grupo Actum Capital, por meio de técnicas, conhecimentos e ferramentas para detectar e explorar fragilidades específicas em um ambiente tecnológico.

4. Medidas de Segurança E Prevenção

Classificação de informações: Classificamos os dados em níveis de confidencialidade, de acordo com a natureza e a criticidade das informações tratadas, restringindo os níveis de acesso e reforçando os mecanismos de controle e segurança de acordo com a criticidade e sensibilidade de cada dado.

Equipamentos e Estrutura: Os equipamentos utilizados para o desenvolvimento das atividades do Grupo Actum Capital devem estar sempre atualizados, regra que inclui sistema operacional, antivírus e firewalls, garantindo assim maior proteção às informações neles inseridas. Ainda, os cuidados se estendem também à infraestrutura onde são armazenados os dados: que possuem cópias de segurança (backups) atualizadas periodicamente, conforme os padrões de segurança mais altos disponíveis no mercado.

Armazenamento de Dados e Computação em Nuvem: Os serviços de armazenamento de dados e computação em nuvem que contratamos passam por uma seleção interna rígida que avalia a necessidade da terceirização do serviço em questão e a confiabilidade técnica do fornecedor analisado, a fim de garantir que ele possua as qualificações de segurança necessárias. Ainda, são cumpridos todos os requisitos previstos na regulamentação específica, em especial a Resolução nº 4.658/2018 do Conselho Monetário Nacional.

Obtenção de Credenciais e Gerenciamento de Acesso: Os nossos colaboradores e prestadores de serviço assumem rígidos compromissos de confidencialidade e compliance ao obterem as credenciais que dão acesso aos nossos dados confidenciais ou a dados classificados como sensíveis pelo Grupo Actum Capital. Estas credenciais, por sua vez, são atualizadas periodicamente, em conformidade com as regulações e normas aplicáveis. Ainda, o acesso aos dados é restringido a menor permissão e privilégio possíveis, possuindo o Grupo Actum Capital capacidade para monitorar e registrar o acesso a dados classificados como sensíveis, sendo exigida a mesma garantia de seus prestadores de serviço.

Capacitação e Atualização: Os nossos colaboradores passam por treinamentos periódicos referentes à prevenção e resposta à incidentes, bem como de melhores práticas de segurança cibernética, sendo realizadas ainda, avaliações buscando atingir o maior comprometimento de todos os nossos colaboradores. Além disso, disponibilizamos canais internos pelos quais os colaboradores possam encaminhar denúncias e suspeitas de fragilidades e violações de segurança cibernética, a fim de agilizar assim a resposta do time especializado a eventuais incidentes.

5. Incidentes de Segurança

Visando garantir a continuidade de nossas atividades em caso de eventuais incidentes de segurança cibernética, realizamos, constantemente, testes de continuidade de negócios, a fim de:

- Diagnosticar possíveis falhas em nossos sistemas;
- Garantir que nossos serviços continuem disponíveis;
- Restaurar os serviços o mais breve possível em caso de interrupção; e
- Aperfeiçoar os métodos de armazenamento e gerenciamento de informações e dados dos clientes.

Assim, após a identificação de possíveis fragilidades efetuamos todas as adequações e alterações necessárias para que a nossa segurança seja mantida.

Caso seja identificado incidente de segurança cibernética o time de resposta deverá ser acionado de acordo a criticidade do incidente.

Na ocorrência de incidentes relevantes, a alta administração e a Supervisão de Relações com o Mercado e Intermediários(SMI) da CVM, serão comunicados após confirmado a materialização do incidente relevante, em toda a sua extensão, e estabelecido planos de ação para mitigá-lo.

6. Disposições Finais

Este Política será revisada, no mínimo, anualmente. Não obstante as revisões estipuladas, poderá ser alterado sem aviso prévio e sem periodicidade definida em razão de circunstâncias que demandem tal providência.

Esta Política se aplica ao Grupo Actum Capital.

A área de *compliance* informará oportunamente aos Membros sobre a entrada em vigor de nova versão deste documento e a disponibilizará na página da Gestora na rede mundial de computadores.

Esta Política revoga todas as versões anteriores e passa a vigorar na data de sua aprovação.