Autêntico Capital

Política de Segurança da Informação e Segurança Cibernética

Ficha Técnica

Título:	Política de Segurança da Informação e Segurança Cibernética
Área Responsável:	Compliance e Tecnologia da Informação
Descrição:	Dispõe sobre a atividade, conceitos, diretrizes e responsabilidades sobre os principais aspectos relacionados à segurança da informação e segurança cibernética, visando preservar a confidencialidade, integridade, disponibilidade e conformidade de todas as informações sob gestão do AUTÊNTICO CAPITAL. Este documento revoga todas as versões anteriores e passa a vigorar na data de atualização.
Data de Atualização:	14/10/2024
Versão:	2024.1.0

Sumário

1. Objetivo

A Política de Segurança da Informação visa esclarecer os procedimentos adotados pela Autêntico Capital Ltda. ("AUTÊNTICO CAPITAL" ou "GESTORA"), para garantir a proteção dos dados de sua propriedade e/ou responsabilidade, no desempenho de suas atividades.

2. Regulamentação Aplicável

- Resolução CVM nº 21/21;
- Código ANBIMA de Administração de Recursos de Terceiros;
- Guia Anbima de Cibersegurança e ANBIMA – Regras e Procedimentos de Deveres Básicos;
- Lei Geral de Proteção de Dados Pessoais, Lei nº 13.709/2018 e alterações.

3. Abrangência

As disposições definidas nesta Política de Segurança da Informação e Segurança Cibernética, devem ser aplicadas a todos os Colaboradores e prestadores de serviços ("colaboradores") que possuam acesso às dependências e/ou que tenham acesso a qualquer tipo de ativo de informação que pertença, ou que estejam sob a responsabilidade da AUTÊNTICO CAPITAL.

4. Divulgação, Vigência e Validade

A Política de Segurança da Informação e Segurança Cibernética, normas e procedimentos relativos ao tratamento dos ativos de informação e/ou dados sigilosos são apresentados aos Colaboradores, com o propósito de desenvolver e manter uma efetiva conscientização de segurança, assim como promover o seu fiel cumprimento. A presente Política será divulgada por intermédio de mensagem eletrônica (e-mail).

A presente Política entra em vigor na data de sua publicação e deverá ser revisto e, se necessário, atualizado pelo Compliance no mínimo a cada 24 meses (vinte e quatro meses). Serão utilizadas como base para sua atualização as legislações, instruções normativas e regulamentações vigentes na data da sua revisão.

5. Ativos de Informação

A AUTÊNTICO CAPITAL considera como ativos de informação todas as informações, disponíveis em qualquer meio, utilizadas ou manipuladas nas operações da empresa, bem como todos os sistemas, equipamentos e instalações onde estas informações são manuseadas ou armazenadas.

As informações podem ser apresentadas nas mais distintas formas escritas, faladas, transmitidas, digitadas, armazenadas ou processadas em qualquer equipamento, papel, telefone, programa de computador, base de dados ou outro meio existente. Seja qual for o estado ou o meio do qual a informação seja apresentada ou compartilhada, ela deverá estar sempre protegida adequadamente, de acordo com as normas definidas nesta Política.

Para que não haja dúvidas, a AUTÊNTICO CAPITAL define como ativos de informação os seguintes itens:

- As informações criadas, processadas, acessadas, manuseadas ou armazenadas em qualquer meio ou sistema de informação da gestora;
- Os computadores, equipamentos, softwares, banco de dados, redes de comunicações e serviços de tecnologia utilizados pela empresa em suas operações, ou qualquer outro recurso, informático ou não, que seja utilizado nas atividades da empresa onde haja manipulação ou armazenamento de informações;
- As instalações em que estão localizados os equipamentos, sistemas, documentos ou informações da gestora;
- Processos e controles internos que sejam parte da rotina das áreas de negócio da AUTÊNTICO CAPITAL; e
- Governança da Gestão de Risco quanto às ameaças e planos de ação, de contingência e de continuidade de negócios.

6. Segurança da Informação

A Segurança da Informação nada mais é que um conjunto de diretrizes que definem formalmente as regras, os direitos e deveres de todos os colaboradores, visando à proteção adequada dos que compartilham a informação. Define as atribuições de cada um dos profissionais em relação à segurança dos recursos com os quais trabalham, além disso, deve prever o que pode ser feito e o que será considerado inaceitável.

Os princípios básicos da segurança da informação são: confidencialidade, integridade e disponibilidade das informações. Outras características são: irretratabilidade, autenticação e o controle de acesso. Os benefícios são evidentes ao reduzir os riscos com vazamentos, fraudes, erros, uso indevido, sabotagens, roubo de informações e diversos outros problemas que possam comprometer esses princípios básicos.

Dessa forma, os princípios de segurança da informação, cujo objetivos constituem a preservação da propriedade da informação, notadamente sua confidencialidade, integridade e disponibilidade, permitindo o uso e compartilhamento de forma controlada, bem como o monitoramento e tratamento de incidentes provenientes de ataques cibernéticos.

A AUTÊNTICO CAPITAL envidará os melhores esforços no sentido de assegurar os pilares da segurança da informação:

- Confidencialidade: Processo pelo qual a informação é disponível de forma controlada com base em nível de permissão de acesso. Ameaça à segurança acontece quando há descuido ou possível quebra da confidencialidade das senhas de acesso à rede.
- Integridade: Processo pelo qual garante-se a veracidade da informação, e que esta não seja afetada por alterações indevidas ou imprevistas.
- Disponibilidade: Processo pelo qual a informação está disponível para pessoas autorizadas, quando necessário.
- Acesso Controlado: O acesso dos usuários à informação é restrito e controlado, significando que só as pessoas que devem ter acesso a uma determinada informação, tenham esse acesso.
- Finalidade: independentemente da forma apresentada ou do meio pelo qual é compartilhada ou armazenada, a informação deve ser utilizada unicamente para a finalidade para a qual foi autorizada.
- Necessidade: garantir que cada Colaborador tenha acesso exclusivamente às informações necessárias ao desempenho de suas atribuições.

7. Gerenciamento de Segurança Cibernética

A Segurança Cibernética constitui-se da preservação das propriedades da informação, notadamente sua confidencialidade, integridade e disponibilidade, permitindo o uso e o compartilhamento da informação de forma controlada, bem como do monitoramento e tratamento de incidentes provenientes de ataques cibernéticos. 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:

- obter recursos financeiros;
- roubar e manipular informações;
- obter informações privilegiadas;
- sabotagem à instituição;
- disseminar falsas notícias; e
- disseminar o caos.

A segurança cibernética deve garantir:

- a segurança dos sistemas e dos bancos de dados;

- o gerenciamento das pessoas autorizadas;
- a segurança dos sistemas e informações que estão na nuvem;
- a segurança para todos os dispositivos/equipamentos; e
- o planejamento da continuidade do negócio; o treinamento constante do usuário final, com o objetivo de minimizar a vulnerabilidade da organização.

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

- risco de imagem;
- risco de continuidade do negócio; e
- prejuízos financeiros.

7.1 – Classificação da Informação

Para que se possam prevenir eventuais ataques cibernéticos e vazamento de informações, primeiro deve-se definir quais informações são as de maior sensibilidade para GESTORA, assim como aquelas que teriam o maior impacto financeiro, operacional e reputacional para AUTÊNTICO CAPITAL, em caso de incidente de segurança.

Deste modo, a AUTÊNTICO CAPITAL segrega as informações geradas pela GESTORA, aperfeiçoando a implementação de processos e o devido manuseio, armazenamento, transporte e descarte destas informações.

Todas as informações seguem uma classificação de segurança, de maneira a serem adequadamente protegidas quanto ao seu acesso e uso, sendo que, para aquelas consideradas de alta criticidade, são necessárias medidas especiais de tratamento. A classificação das informações deverá seguir a seguinte ordem:

- Pública: É uma informação da AUTÊNTICO CAPITAL ou de seus clientes com linguagem e formato dedicado à divulgação ao público em geral, sendo seu caráter informativo, comercial ou promocional. É destinada ao público externo ou ocorre devido ao cumprimento de legislação vigente que exija publicidade.
- Interna: É uma informação da AUTÊNTICO CAPITAL que ela não tem interesse em divulgar, onde o acesso por parte de indivíduos externos à empresa deve ser evitado. Caso esta informação seja acessada indevidamente, poderá causar danos à imagem da organização, porém, não com a mesma magnitude de uma informação confidencial. Pode ser acessada sem restrições por todos os empregados e prestadores de serviços da AUTÊNTICO CAPITAL.
- Confidencial: É uma informação crítica para os negócios da AUTÊNTICO CAPITAL ou de seus clientes. A divulgação não autorizada dessa informação pode causar impactos de ordem financeira, de imagem, operacional ou, ainda, sanções administrativas, civis e criminais à AUTÊNTICO CAPITAL ou aos seus clientes. É sempre restrita a um grupo específico de pessoas, podendo ser este composto por empregados, clientes e/ou fornecedores.
- Privilegiada: É a informação relevante ainda não divulgada publicamente e que seja obtida de forma privilegiada (em decorrência da relação profissional ou pessoal mantida com um cliente, com pessoas vinculadas a empresas analisadas ou investidas ou com terceiros). As informações privilegiadas devem ser mantidas em sigilo por todos que a elas tiverem acesso, seja em decorrência do exercício da atividade profissional ou de relacionamento pessoal.
- Restrita: É toda informação que pode ser acessada somente por usuários da AUTÊNTICO CAPITAL explicitamente indicado pelo nome ou por área a que pertence. A divulgação não autorizada dessa informação pode causar sérios danos ao negócio e/ou comprometer a estratégia de negócio da organização.

As informações digitais da AUTÊNTICO CAPITAL são classificadas de acordo com os seguintes critérios:

- Quaisquer informações e/ou dados que a AUTÊNTICO CAPITAL teve acesso ou conhecimento por ser de domínio público ("Informação Pública");
- Quaisquer informações e/ou dados que não estejam sujeitas a compromissos ou acordos de confidencialidade;
- Quaisquer informações e/ou dados que tenham a obrigatoriedade de divulgação por lei ou autoridade competente;
- Quaisquer informações que venham a ter a obrigatoriedade de divulgação por lei ou autoridade competente, mas o termo legal ainda não foi iniciado ou findado (Ex. Data de Divulgação);
- Todas as Informações Confidenciais, a saber: o know-how, técnicas, cópias, diagramas, modelos, amostras, programas de computador, informações técnicas, financeiras, estatísticas, logísticas ou relacionadas às estratégias de investimento ou comerciais, incluindo saldos, extratos e posições de clientes e/ou dos fundos geridos pela AUTÊNTICO CAPITAL
- operações estruturadas, demais operações e seus respectivos valores, analisadas ou realizadas para os fundos de investimento e carteiras geridas pela AUTÊNTICO CAPITAL; e
- estruturas, planos de ação, relação de clientes, contrapartes comerciais, fornecedores e prestadores de serviços, bem como informações estratégicas, mercadológicas ou de qualquer natureza relativas às atividades da AUTÊNTICO CAPITAL e/ou de seus sócios e clientes.

A partir da definição acima, a AUTÊNTICO CAPITAL se empenhará para manter controles, conforme o nível de criticidade das informações e dados, sendo certo de que a prioridade será escalonada na seguinte ordem de relevância.

Nenhuma informação da AUTÊNTICO CAPITAL classificada como confidencial, privilegiada e restrita pode ou deve ser discutida em locais inapropriados, como lugares públicos ou fechados, na presença de terceiros ou pessoas não diretamente relacionadas ao assunto, ou adiante daqueles sem autorização para conhecimento dessas informações. Todos os Colaboradores estão proibidos de fazer transitar, por qualquer meio, qualquer informação que não seja de domínio público, fora dos procedimentos estabelecidos por esta política e em normas específicas da AUTÊNTICO CAPITAL para trânsito de informações.

Qualquer informação sobre a GESTORA ou de qualquer natureza relativa às atividades da AUTÊNTICO CAPITAL e aos sócios e clientes, obtida em decorrência do desempenho das atividades normais dos Colaboradores, só poderá ser fornecida ao público, mídia ou a demais órgãos caso autorizado pelo Compliance, apontado nos termos do Código de Ética e Conduta da AUTÊNTICO CAPITAL.

A gestão dessas informações é realizada através de um processo de melhoria contínua, partindo dos seguintes mecanismos de supervisão:

- Classificação de informações: conforme mencionado acima o acesso é restringido e são reforçados 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 da AUTÊNTICO 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;
- 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;

- Gerenciamento de Acesso: Os acessos dados são restringidos a menor permissão e privilégio possíveis, possuindo a AUTÊNTICO CAPITAL a capacidade para monitorar e registrar o acesso a dados classificados como dados pessoais sendo exigida a mesma garantia de seus colaboradores e terceiros contratados, conforme Lei Geral de Proteção de Dados (Lei nº 13.709); e
- Capacitação e Atualização: Os colaboradores e os terceiros contratados passam por treinamentos periódicos referentes à prevenção e resposta à incidentes, bem como de melhores práticas de segurança da informação e cibernética, sendo realizadas ainda, avaliações buscando atingir o maior comprometimento de todos os nossos colaboradores.

Todos os Colaboradores, ao tomarem conhecimento de qualquer incidente referente à segurança da informação e cibernética, devem notificar o fato, imediatamente ao Compliance, via e-mail.

7.2 – Avaliação dos riscos

No exercício das suas atividades, a AUTÊNTICO CAPITAL poderá estar sujeita a riscos cibernéticos que ameacem a confidencialidade, a integridade e a disponibilidade dos dados e dos sistemas de informação utilizados. Entre os riscos mais comuns estão:

- Malwares: softwares desenvolvidos para corromper computadores e redes:
- Vírus: software que causa danos à máquina, rede, à outros softwares e bancos de dados.
- Cavalo de Troia: aparece dentro de outro software e cria uma porta para a invasão do computador.
- Spyware: software malicioso para coletar e monitorar o uso de informações.
- Ransomware: software malicioso que bloqueia o acesso a sistemas e bases de dados, solicitando um resgate para que o acesso seja reestabelecido.
- Engenharia social: métodos de manipulação para obter informações confidenciais, como senhas, dados pessoais e número de cartão de crédito:
- Pharming: direciona o usuário para um site fraudulento, sem o seu conhecimento.
- Phishing: links transmitidos por e-mails, simulando ser uma pessoa ou empresa confiável que envia comunicação eletrônica oficial para obter informações confidenciais.
- Vishing: simula ser uma pessoa ou empresa confiável e, por meio de ligações telefônicas, tenta obter informações confidenciais.
- Smishing: simula ser uma pessoa ou empresa confiável e, por meio de mensagens de texto, tenta obter informações confidenciais.
- Acesso pessoal: pessoas localizadas em lugares públicos, como bares, cafés e restaurantes, que captam qualquer tipo de informação que possa ser utilizada posteriormente para um ataque.
- Ataques de DDoS (distributed denial of servi ce) e botnets: ataques visando negar ou atrasar o acesso aos serviços ou sistemas da instituição; no caso dos botnets, o ataque vem de um grande número de computadores infectados utilizados para criar e mandar spam ou vírus, ou inundar uma rede com mensagens resultando na negação de serviços.
- Invasões (advanced persistent threats): ataques realizados por invasores sofisticados, utilizando conhecimentos e ferramentas para detectar e explorar fragilidades específicas em um ambiente tecnológico.

Com base na informação acima, a AUTÊNTICO CAPITAL avalia e define o plano estratégico de prevenção e acompanhamento para a mitigação ou eliminação do risco, assim como as eventuais modificações necessárias e o plano de retomada das atividades normais e restabelecimento da segurança devida.

Os possíveis impactos dependem ainda da rápida detecção e resposta após a identificação do ataque. Uma vez definidos os riscos, ações de prevenção e proteção deverão ser tomadas de acordo com esta política e conforme orientação do Diretor de Compliance.

A avaliação dos riscos e as ações de prevenção inerentes às atividades desempenhadas pela AUTÊNTICO CAPITAL estão descritas no Anexo I da presente Política.

7.3 – Proteção da informação e segurança cibernética

Os sistemas de informação da AUTÊNTICO CAPITAL contam com proteção dos ativos de informação contra ameaças internas e externas, intencionais ou acidentais, com os objetivos de assegurar a continuidade do negócio e de minimizar o impacto de violações de segurança. A estrutura de informática e de comunicação é constituída essencialmente pelos recursos especificados a seguir:

- Firewall de Rede. Trata da segurança e proteção da rede.
- Antivírus. Prevenção, contenção e mitigação do impacto de software malicioso na rede, em aplicações e em outros sistemas que poderiam impactar a confidencialidade, a integridade ou a disponibilidade da informação.
- Segurança da informação. Abordagem para tratar e responder aos incidentes cibernéticos e de segurança da informação.
- Computação em nuvem. Requisitos de computação em "nuvem" para atender às políticas, normas e aos procedimentos de proteção da informação, além da implementação da infraestrutura, da plataforma e dos serviços criados para dar suporte à estrutura, aos sistemas e aos dispositivos de computação distribuídos em tais ambientes.
- Sistemas de backup. Os meios de armazenamento em servidores em nuvem, o espelhamento das informações em uma segunda nuvem configurados para recuperação e disponibilização nas condições originalmente padronizadas de armazenamento e consumo das informações.
- Redundância em link de internet. Para garantir a continuidade de todas as operações, pelo menos 2 (duas) operadoras são conectadas aos provedores para evitar a indisponibilidade de conexão em caso de caso falhas ou interrupções.
- Redundância na telefonia. A utilização do sistema de telefonia VOIP permitirá as comunicações por rede de fibra óptica de internet. Caso essa rede fique inoperante, o sistema automaticamente acionará a rede 4G (rede móvel), garantindo a continuidade das operações.
- Permissão e acesso. Identificação e autenticação dos Colaboradores para acesso controlado à rede e aos sistemas obedecendo a critérios de concessão de informações de acordo com o perfil de cada usuário.
- Bloqueio e cancelamento de acessos. Bloqueios e cancelamentos de acessos efetuados, quando do desligamento de profissionais ou pela área de Compliance, para o cumprimento de regulamentações ou com foco na mitigação de riscos.
- Acesso remoto. Proteção das informações exigidas para prover acesso remoto seguro, quando autorizado, a Colaboradores e prestado redes de serviço da AUTÊNTICO CAPITAL.
- Descarte. Descarte seguro de mídias e documentos físicos.

7.4 – Contratação de Serviços de Processamento e Armazenamento de Dados em Nuvem

A AUTÊNTICO CAPITAL irá verificar a capacidade e o potencial prestador de serviço, na contratação de serviços de processamento e armazenamento de dados em nuvem, incluindo, no mínimo:

- O acesso da AUTÊNTICO CAPITAL aos dados e às informações a serem processados ou armazenados pelo prestador de serviço;
- A confidencialidade, a integridade, a disponibilidade e a recuperação das informações e dados processados ou armazenados pelo prestador de serviço;
- A sua aderência a certificações exigidas pela AUTÊNTICO CAPITAL ou reguladores para a prestação do serviço a ser contratado, caso aplicável;
- O provimento de informações e de recursos de gestão adequados ao monitoramento dos serviços a serem prestados;
- A qualidade dos controles de acesso voltados à proteção dos dados e das informações dos clientes, funcionários, colaboradores e terceiros relevantes.

Adicionalmente, a AUTÊNTICO CAPITAL poderá utilizar o questionário de due diligence para contratação de serviço de processamento e armazenamento de dados e de computação em nuvem, no país ou no exterior, disponibilizado no site da ANBIMA.

7.5 – Comportamento seguro

Além dos sistemas de informação, é fundamental que os Colaboradores adotem comportamentos seguros em relação ao manuseio e tratamento dos dados e das informações. Os Colaboradores deverão:

- Compreender situações de risco ou ameaças que possam comprometer a segurança dos dados, tais como e-mails de phishing, acesso a sites maliciosos, vírus de computador em geral.
- Não instalar ou utilizar qualquer tipo de software sem a autorização prévia da AUTÊNTICO CAPITAL.
- Não fornecer as credenciais de acesso a terceiros.
- Utilizar senhas com alto nível de segurança.
- Evitar o acesso de informações em ambientes públicos.
- Notificar imediatamente o Compliance quando houver roubo ou extravio de materiais ou equipamentos contendo informações confidenciais.

7.6 – Monitoramento

A AUTÊNTICO CAPITAL possui mecanismos de monitoramento das ações de proteção implementadas, para garantir seu bom funcionamento e sua efetividade.

Nesse sentido, a AUTÊNTICO CAPITAL mantém inventários atualizados de hardware e software, bem como realiza verificações periódicas, no intuito de identificar elementos estranhos à AUTÊNTICO CAPITAL, como computadores não autorizados ou softwares não licenciados.

Além disso, a AUTÊNTICO CAPITAL mantém os sistemas operacionais e softwares de aplicação sempre atualizados, instalando as atualizações sempre que forem disponibilizadas. As rotinas de backup são monitoradas diariamente, com a execução de testes regulares de restauração dos dados.

Ainda, a AUTÊNTICO CAPITAL analisa regularmente os logs e as trilhas de auditoria criados, de forma a permitir a rápida identificação de ataques, sejam internos ou externos.

7.7 – Plano de resposta

Caso seja identificado um potencial incidente relacionado à segurança cibernética, o Diretor de Compliance deverá ser imediatamente comunicado.

Num primeiro momento, o Diretor de Compliance se reunirá com os demais diretores da AUTÊNTI-

CO CAPITAL para compreender o evento ocorrido, os motivos e as consequências imediatas, bem como a gravidade da situação.

Caso os diretores avaliem que o incidente ocorrido pode gerar danos iminentes à AUTÊNTICO CAPITAL, serão tomadas, em conjunto com os assessores de tecnologia da informação da Gestora, as medidas imediatas de cibersegurança cabíveis, que podem incluir a redundância de TI, redirecionamento das linhas de telefone para os celulares, instrução do provedor de telefonia para que desvie linhas de dados e e-mails, entre outros.

Na hipótese de o incidente comprometer, dificultar ou mesmo impedir a continuidade das operações da AUTÊNTICO CAPITAL, serão observados os procedimentos previstos no plano de continuidade do negócio.

Além disso, os diretores avaliarão a pertinência da adoção de medidas como (i) registro de boletim de ocorrência ou queixa-crime; (ii) comunicação do incidente aos órgãos regulatórios e autorregulatórios; (iii)consulta com advogado para avaliação dos riscos jurídicos e medidas judiciais cabíveis para assegurar os direitos da AUTÊNTICO CAPITAL.

7.8 – Uso De Equipamentos, Sistemas, Segurança e Confidencialidade

Os acessos físicos são controlados pelo Compliance e orientados de forma a garantir que apenas pessoas autorizadas possuam o efetivo acesso às instalações e equipamentos que pertençam e/ou que sejam utilizados pela Gestora.

Os acessos às informações (dados) e aos ambientes lógicos (sistemas) são controlados, de forma a garantir o efetivo acesso apenas de pessoas autorizadas, sendo certo que tal restrição/segregação será feita em relação a: (i) área/atividade, (iii) cargo/nível hierárquico e (iii) equipe.

Cada colaborador e prestador de serviço é responsável por manter o controle e sigilo de todas os tipos de informações da AUTÊNTICO CAPITAL, citados nesta política, bem como em especial atenção para as informações confidenciais e privilegiadas que lhes tenham sido confiadas em virtude do exercício de suas atividades profissionais, excetuadas as hipóteses permitidas em lei e que estão sob sua responsabilidade.

Conforme estabelecido pela AUTÊNTICO CAPITAL, todos os Colaboradores e prestadores de serviço contratados devem assinar, de forma manual ou eletrônica, o Termo Compromisso, documento anexo ao Manual de Compliance comprometendo-se a observar integralmente os termos desta Política de Segurança da Informação e Segurança Cibernética.

Estão dispensados de assinar o Termo de Compromisso os prestadores de serviços contratados, que em seu contrato de prestação de serviço haja uma cláusula de confidencialidade.

8. Governança e Responsabilidades

A AUTÊNTICO CAPITAL se utiliza de um profissional de TI, responsável por administrar a área de Tecnologia da Informação – TI e executar as atividades nas funções fundamentais e rotinas da área, sendo de responsabilidade da Diretoria de Compliance o gerenciamento e controle de qualidade do serviço de TI.

8.1 – Diretoria Executiva

A Diretoria Executiva é o órgão máximo de de liberação da GESTORA. Sua atuação é pautada pelo compromisso da instituição com as melhores práticas na governança e no processo de Segurança da Informação, melhorando continuamente esta Política, sua governança, seus processos, seus procedimentos, os controles internos e a cultura organizacional sobre o tema. Neste sentido, são suas atribuições:

- Estabelecer e revisar as diretrizes desta Política, no mínimo, anualmente;
- Prover recursos para que toda equipe atuante no processo possa alcançar seus objetivos;

- Zelar pela prevenção incidentes relacionados à Segurança da Informação; e
- Avaliar a efetividade desta Política e dos procedimentos relacionados à Segurança da Informação.

8.2 – Comitê de Riscos e Operações

É da alçada do Comitê de Riscos e Operações:

- Aprovar os manuais de procedimentos que envolvem a Segurança da Informação;
- Analisar as demandas levadas a pauta das reuniões do Comitê de Risco e Compliance emitindo pareceres e decisões de acordo com esta Política e com a legislação aplicável.

8.3 – Tecnologia da Informação

É de responsabilidade da área de Tecnologia da Informação:

- A manutenção contínua do ambiente tecnológico seguro e que suporte a operação da GESTORA;
- Oferecer suporte técnico e operacional às demais áreas nos assuntos relacionados à Segurança da Informação; e
- Manter seus processos aderentes às disposições estabelecidas nesta Política.

8.4 – Compliance

A área de Compliance é responsável por:

- divulgar e dar conhecimento a todos sobre as normas e os procedimentos relativos à Segurança da Informação;
- orientar os Colaboradores de acordo com as regras estabelecidas nesta Política;
- prover treinamento aos Colaboradores com programação permanente e de amplo alcance; e
- executar rotinas de diligência sobre a aderência dos processos estabelecidos nas diretrizes da presente Política.

9. Treinamento e Conscientização

Considerando que o nível de segurança depende da cooperação de todos os colaboradores, e com a finalidade de disseminar a cultura de Segurança da Informação e desta Política é promovido treinamento anual, com o intuito de orientar sobre:

- As responsabilidades e os procedimentos relacionados a cada área de atuação;
- Acessos e limites de uso das informações de forma apropriada; e

Os requerimentos e obrigações de confidecialidade.

10. Proteção de Dados

De acordo com a Lei n° 13.709, de 14 de agosto de 2018 ("LGPD"), a AUTÊNTICO CAPITAL irá sempre atuar na busca de investimento em cibersegurança e implementação de sistemas de compliance efetivos para prevenir, detectar e remediar violações de dados pessoais.

A segurança da informação prevista na LGPD, em relação aos Dados Pessoais, mesmo após seu término, é responsabilidade dos Agentes de Tratamento de Dados Pessoais ou qualquer outra pessoa que intervenha no Tratamento.

A AUTÊNTICO CAPITAL possui Política de LGPD que abrange também os Dados Pessoais que sejam tratados pela GESTORA, e trazem as medidas estabelecidas para a proteção dos dados.

A GESTORA está comprometida em preservar a privacidade de dados pessoais e de dados sensíveis que forem coletados ou aos quais tiver acesso em função do uso do site ou por conta do desempenho de suas atividades, e com o cumprimento das leis e regulamentos em vigor. É importante observar que o escopo da proteção de dados pessoais no âmbito da AUTÊNTICO CAPITAL está, em grande parte, limitado aos dados pessoais de seus Colaboradores e de pessoas físicas e jurídicas com as quais tiver estabelecido relações jurídicas. Também estão abrangidos por esta proteção os dados de candidatos às vagas na GESTO-

RA, de fornecedores e outros com os quais a AUTÊNTICO CAPITAL manteve contato para atender alguma demanda relevante e específica.

A AUTÊNTICO CAPITAL (na qualidade de Controlador) é responsável pela guarda dos Dados Pessoais coletados e armazenados em seus sistemas, sendo que os Dados Pessoais devem ser tratados com base nas hipóteses permitidas na legislação.

Nas hipóteses em que o tratamento de dados não tiver sido previamente mapeado pela AUTÊNTICO CAPITAL, o encarregado deverá ser acionado para definir as providências a serem tomadas para garantir o correto Tratamento dos Dados Pessoais.

As normas de segurança e padrões técnicos para o gerenciamento de riscos de segurança cibernética e para mitigação de riscos estão previstos na presente Política.

Qualquer solicitação em relação ao tratamento de dados pessoais ou de informações específicas relacionadas ao tratamento de dados pessoais, se faz necessário o envio um e-mail para compliance@autenticocapital.com.br (Favor informar o respectivo e-mail de contato do DPO).

11. Considerações Finais

Todas as dúvidas sobre as diretrizes desta Política podem ser esclarecidas com o Compliance da AUTÊNTICO CAPITAL.

12. Manutenção dos Arquivos

A AUTÊNTICO CAPITAL manterá armazenado todos os arquivos eletronicamente, pertinentes ao processo de Compliance desta política, pelo prazo mínimo de 05 (cinco) anos, conforme legislação vigente.

13. Anexo I

No exercício de suas atividades, a AUTÊNTICO CAPITAL e utiliza primordialmente dos processos e ativos da organização identificados.

Para cada processo/ativo identificado, o Compliance avaliará o risco quanto à ameaça cibernética e à segurança da informação e seu impacto na organização, caso o evento de risco se realize, definindo, assim, as correspondentes ações de prevenção e proteção, conforme mapeamento abaixo:

Processo Ativo	Ameaças	Grau de Exposição	Impacto			Ações de Prevenção e Proteção
			Financeiro	Reputação	Operacional	
Sistemas em "Nuvem"	Malware	Alto	Médio	Médio	Alto	Firewall/antivírus/sistema operacional atualizados, backups diários, provedores de serviço na nuvem de boa reputação; uso de códigos/iniciais e não nomes dos clientes; sistemas com login/perfil de acesso; controle de acesso centralizado e conforme Inventário de Informações; logs de acessos e trilha de auditoria.
	Ataques DDoS	Baixo	Baixo	Baixo	Alto	
	Invasões	Médio	Médio	Médio	Alto	
Servidor de Arquivos Informações Gerais: Documentos	Malware	Médio	Médio	Médio	Alto	Firewall/antivírus/sistema operacional atualizados, backups diários, provedores de serviço na nuvem de boa reputação; controle de acesso centralizado e conforme Inventário de Informações; logs de acessos e trilha de auditoria.
	Ataques DDoS	Baixo	Baixo	Baixo	Médio	
	Invasões	Baixo	Médio	Médio	Alto	
Documentos Físicos Gerais: Pessoa Física Terceiro Contratado Colaborador Outros relevantes	Engenharia Social Acesso a informações restritas	Alto	Baixo	Médio	Médio	Código de Ética e Conduta e Regras e Procedimento de Compliance (treinamento e prática) Política de Mesa Limpa / armazenamento seguro Destruição de documentos segura Acesso restrito ao escritório / segurança Acessos restrito à informação na nuvem conforme controle de acessos definidos.
Trading (e-mail e Telefone)	Engenharia Social Invasão de e-mails	Médio	Baixo	Médio	Baixo	Provedores de e-mail de boa reputação; uso de códigos e contas e não nomes no trading
Comunicação geral (e-mail e telefone)	Engenharia Social Invasão de e-mails	Médio	Baixo	Médio	Baixo	Provedores de e-mail de boa reputação; uso de nomes abreviados, iniciais ou primeiro nome na comunicação
Contratação de Serviços em Nuvem no país e no exterior	Engenharia Social Riscos Cibernéticos	Baixo	Baixo	Baixo	Baixo	Seguir as diretrizes emanadas no documento Regras e Procedimentos de Deveres Básicos – ANBIMA, integrante ao Código AGRT. Questionário DD Cibersegurança, quando aplicável