Manual de regras, procedimentos e descrição dos controles internos

Este Manual da Gauss Capital Gestora de Recursos Ltda. ("Gauss Capital") formaliza e esclarece as regras, os procedimentos e controles internos para fins de **Segurança da Informação e Segurança Cibernética.**

Segurança da Informação e Cibernética

A política de segurança da informação e segurança cibernética leva em consideração diversos riscos e possibilidades considerando o porte, perfil de risco, modelo de negócio e complexidade das atividades desenvolvidas pela Gauss Capital.

A coordenação direta das atividades relacionadas à política de segurança da informação e segurança cibernética ficará a cargo do Diretor de Risco e Compliance, que será responsável inclusive por sua revisão, realização de testes e treinamento dos Colaboradores, conforme aqui descrito.

1. Princípios básicos da segurança da informação

Os seguintes princípios básicos norteiam esta política:

- confidencialidade
- treinamento e conscientização sobre segurança da informação para todos os colaboradores
- testes periódicos dos sistemas de informação

Confidencialidade e controle de acesso
O acesso aos sistemas é liberado com base no princípio da necessidade da informação para a execução da função do colaborador (*need-to-know/need-to-have principle*). O controle é feito por meio dos perfis de acesso, que segregam as funções realizadas pelas diversas áreas. Cada área possui um conjunto de perfis relacionados às suas atividades, e a Gauss Capital dispõe de controles internos para que o acesso seja liberado mediante aprovação da área de Compliance.

Treinamento e conscientização
A Gauss Capital oferece treinamentos periódicos aos quais os colaboradores são submetidos durante o ano, com o objetivo de conscientizá-los sobre confidencialidade das informações, *cyber* segurança, engenharia social, *phishing*, entre outras potenciais ameaças à integridade dos sistemas de informação.

Testes periódicos de segurança
A Gauss Capital dispõe de tecnologias de defesa contra possíveis ataques aos seus sistemas de informação e realiza testes periódicos no sistema disponível na rede mundial de computadores.

Testes são realizados anualmente com os próprios colaboradores, que são submetidos a uma simulação de *phishing*.

2. Identificação de Riscos (*risk assessment*)

No âmbito de suas atividades, a Gauss Capital identificou os seguintes principais riscos internos e externos que precisam de proteção:

- Dados e Informações: as Informações Confidenciais, incluindo informações a respeito de investidores, clientes, Colaboradores e da própria Gauss Capital, operações e ativos investidos pelas carteiras de valores miliários sob sua gestão, e as comunicações internas e externas (por exemplo: correspondências eletrônicas e físicas);

- Sistemas: informações sobre os sistemas utilizados pela Gauss Capital e as tecnologias desenvolvidas internamente e por terceiros;

- Processos e Controles: processos e controles internos que sejam parte da rotina das áreas de negócio e compliance da Gauss Capital;

- Governança da Gestão de Risco: a eficácia da gestão de risco pela Gauss Capital quanto às ameaças e planos de ação, de contingência e de continuidade de negócios.

Ademais, no que se refere especificamente à segurança cibernética, a Gauss Capital identificou as seguintes principais ameaças, em linha com o disposto no Guia de Cibersegurança da ANBIMA:

- Malware – softwares desenvolvidos para corromper computadores e redes (tais como: Vírus, Cavalo de Troia, *Spyware* e *Ransomware*);

- Engenharia social – métodos de manipulação para obter informações confidenciais (*Pharming, Phishing, Vishing, Smishing*, e Acesso Pessoal);

- Ataques de DDoS (distributed denial of services) e botnets: ataques visando negar ou atrasar o acesso aos serviços ou sistemas da instituição;

- 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 no acima, a Gauss 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 reestabelecimento da segurança devida.

3. Ações de Prevenção e Proteção

- Regras Gerais

No tocante à segurança da informação, seguindo o princípio da confidencialidade e do controle de acesso mencionados acima, o acesso aos sistemas é liberado com base no princípio da necessidade da informação para a execução da função do colaborador (*need-to-know/need-to-have principle*),

aplicando-se referido princípio, inclusive no que se refere às informações confidenciais, reservadas ou privilegiadas. O controle é feito por meio dos perfis de acesso, que segregam as funções realizadas pelas diversas áreas. Cada área possui um conjunto de perfis relacionados às suas atividades, e a Gauss Capital dispõe de controles internos para que o acesso seja liberado mediante aprovação.

É proibido que os Colaboradores façam cópias (físicas ou eletrônicas) ou imprimam os arquivos utilizados, gerados ou disponíveis na rede da Gauss Capital e circulem em ambientes externos à Gauss Capital com estes arquivos, uma vez que tais arquivos contêm informações que são consideradas como informações confidenciais. As exceções devem ser autorizadas pelo superior hierárquico ou pelo Diretor de Risco e Compliance.

A proibição acima referida também não se aplicará quando as cópias (físicas ou eletrônicas) ou a impressão dos arquivos forem indispensáveis e em prol da execução e do desenvolvimento dos negócios e dos interesses da Gauss Capital. Nestes casos, o Colaborador que estiver na posse e guarda da cópia ou da impressão do arquivo que contenha a informação confidencial será o responsável direto por sua boa conservação, integridade e manutenção de sua confidencialidade.

Em consonância com as normas internas acima, os Colaboradores devem se abster de utilizar pen-drivers, fitas, discos ou quaisquer outros meios que não tenham por finalidade a utilização exclusiva para o desempenho de sua atividade na Gauss Capital. É proibida a conexão de equipamentos na rede da Gauss Capital que não estejam previamente autorizados pela área de informática (ainda que terceirizada) e pelo Diretor de Risco e Compliance.

A utilização dos ativos e sistemas da Gauss Capital, incluindo computadores, telefones, internet, e-mail e demais aparelhos se destina prioritariamente a fins profissionais, devendo, portanto, evitar o uso indiscriminado deles para fins pessoais.

O envio ou repasse por e-mail de material que contenha conteúdo discriminatório, preconceituoso, obsceno, pornográfico ou ofensivo é também terminantemente proibido, bem como o envio ou repasse de e-mails com opiniões, comentários ou mensagens que possam difamar a imagem e afetar a reputação da Gauss Capital.

O recebimento de e-mails muitas vezes não depende do próprio Colaborador, mas espera-se bom senso de todos para, se possível, evitar receber mensagens com as características descritas previamente. Na eventualidade do recebimento de mensagens com as características acima descritas, o Colaborador deve apagá-las imediatamente, de modo que estas permaneçam o menor tempo possível nos servidores e computadores da Gauss Capital, bem como avisar prontamente o Diretor de Risco e Compliance.

A visualização de sites, blogs, fotologs, webmails, entre outros, que contenham conteúdo discriminatório, preconceituoso sobre origem, etnia, religião, classe social, opinião política, idade, sexo, ou deficiência física, obsceno, pornográfico ou ofensivo é terminantemente proibida.

- Acesso Escalonado ao Sistema

O acesso como "administrador" de área de desktop será limitado aos usuários aprovados pelo Diretor de Risco e Compliance, com isso, serão determinados privilégios/credenciais e níveis de acesso de usuários apropriados para os Colaboradores.

A Gauss Capital, ademais, mantém diferentes níveis de acesso a pastas e arquivos eletrônicos, notadamente aqueles que contemplem Informações Confidenciais, de acordo com as funções e responsabilidades dos Colaboradores e pode monitorar o acesso dos Colaboradores a tais pastas e arquivos com base na senha e login disponibilizados.

A implantação destes controles é projetada para limitar a vulnerabilidade dos sistemas da Gauss Capital em caso de violação.

- Senha e Login

A senha e login para acesso aos dados contidos em todos os computadores, bem como nos e-mails que também possam ser acessados via webmail, devem ser conhecidas pelo respectivo usuário do computador e são pessoais e intransferíveis, não devendo ser divulgadas para quaisquer terceiros.

Dessa forma, o Colaborador pode ser responsabilizado inclusive caso disponibilize a terceiros a senha e login acima referidos, para quaisquer fins.

- 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.

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 seu superior hierárquico ou o Diretor de Risco e Compliance.

- Acesso Remoto

A Gauss Capital permite o acesso remoto pelos Colaboradores, de acordo com a seguinte regra: todos os acessos remotos são permitidos mediante pedido prévio e por e-mail ao Diretor de Risco e Compliance, que ficará responsável por autorizar. Os acessos remotos darão permissões de acesso aos mesmos sistemas, pastas e arquivos observados no escritório da gestora. O Diretor de Risco e Compliance, junto com a área de TI, será responsável por validar tais acessos.

O acesso remoto será feito através de portal de serviço hospedado em Cloud e o acesso não permitirá a troca de dados fora do ambiente da rede da gestora.

- Controle de Acesso

O acesso de pessoas estranhas à Gauss Capital a áreas restritas somente é permitido com a autorização expressa de Colaborador autorizado pelo Diretor de Risco e Compliance sempre acompanhado, sendo certo que a Gauss Capital mantém sistema de acesso por código para o servidor de dados e CPD.

Somente os Diretores e os colaboradores autorizados têm acesso ao CPD, ademais qualquer prestador de serviço só poderá entrar no CPD acompanhado por algum colaborador da Gestora devidamente autorizado por um Diretor.

O acesso à rede de informações eletrônicas conta com a utilização de servidores exclusivos da Gauss Capital e serviço de armazenamento de dados em nuvem, em conta dedicada, que não poderão ser compartilhados com outras empresas responsáveis por diferentes atividades no mercado financeiro e de capitais.

Tendo em vista que a utilização de computadores, telefones, internet, e-mail e demais aparelhos se destina exclusivamente para fins profissionais, como ferramenta para o desempenho das atividades dos Colaboradores, a Gauss Capital monitora a utilização de tais meios.

- Firewall, Software, Varreduras e Backup

A Gauss Capital utilizará um hardware de firewall projetado para evitar e detectar conexões não autorizadas e incursões maliciosas. O Diretor de Risco e Compliance será responsável por determinar o uso apropriado de firewalls (por exemplo, perímetro da rede).

A Gauss Capital manterá proteção atualizada contra malware nos seus dispositivos e software antivírus projetado para detectar, evitar e, quando possível, limpar programas conhecidos que afetem de forma maliciosa os sistemas da empresa (por exemplo, vírus, *worms*, *spyware*).

Como parte de suas rotinas regulares de verificação, a área de TI realiza um escaneamento completo dos sistemas da Gauss Capital, ao menos 1 (uma) vez por semana, buscando identificar e eliminar as ameaças.

A Gauss Capital também manterá e testará regularmente medidas de backup consideradas apropriadas pelo Diretor de Risco e Compliance. As informações da Gauss Capital são atualmente objeto de backup diário com o uso de computação na nuvem.

Para maiores informações, vide Plano de Contingência e Continuidade, arquivado na sede da Gauss Capital.

Observado disposto no presente Manual e nas demais políticas da Gauss Capital, as seguintes condutas devem ser observadas pelos Colaboradores da Gauss Capital:

- é expressamente proibida a instalação de softwares não homologados pelo departamento de informática, bem como fazer downloads pela Internet;
- é expressamente proibida a instalação de qualquer hardware que não esteja homologado pelo departamento de informática (Ex.: scanner, câmera fotográfica, etc.);
- não utilização de disquetes, CDs, pen drives ou quaisquer outras mídias, sem prévia autorização do Diretor de Risco e Compliance, e quando necessário da devida verificação pelo departamento de informática;
- não abertura de e-mail de remetente duvidoso ou desconhecido, principalmente os que tiverem anexos ou executáveis;
- manutenção de sigilo das senhas de acesso à rede e Internet. Todo usuário terá uma pasta no servidor da Gauss Capital sempre na rede corporativa, onde devem ser gravados seus arquivos.

Qualquer arquivo que não for salvo neste local, não terá garantia de backup (cópia de segurança); e

- comunicação ao departamento de informática, quando da instalação de softwares específicos

4. Treinamento e Conscientização dos Colaboradores

Conforme já disposto acima, a Gauss Capital oferece treinamentos aos seus colaboradores com o objetivo de conscientizá-los sobre a confidencialidade das informações, *cyber* segurança, engenharia social, *phishing*, entre outras potenciais ameaças à integridade dos sistemas de informação. Referido treinamento é realizado anualmente.

5. Plano de Identificação e Resposta

- Identificação de Suspeitas

Qualquer suspeita de violação, acesso não autorizado, outro comprometimento da rede ou dos dispositivos da Gauss Capital (incluindo qualquer violação efetiva ou potencial), ou ainda no caso de vazamento de quaisquer Informações Confidenciais, mesmo que de forma involuntária, deverá ser informada ao Diretor de Risco e Compliance prontamente. O Diretor de Risco e Compliance determinará quais membros da administração da Gauss Capital e, se aplicável, de agências reguladoras e de segurança pública, deverão ser notificados.

Ademais, o Diretor de Risco e Compliance determinará quais clientes ou investidores, se houver, deverão ser contatados com relação à violação.

- Procedimentos de Resposta

O Diretor de Risco e Compliance responderá a qualquer informação de suspeita de violação, acesso não autorizado ou outro comprometimento da rede ou dos dispositivos da Gauss Capital de acordo com os critérios abaixo:

(i) Avaliação do tipo de incidente ocorrido (por exemplo, infecção de malware, intrusão da rede, furto de identidade), as informações acessadas e a medida da respectiva perda;

(ii) Identificação de quais sistemas, se houver, devem ser desconectados ou de outra forma desabilitados;

(iii) Determinação dos papéis e responsabilidades do pessoal apropriado;

(iv) Avaliação da necessidade de recuperação e/ou restauração de eventuais serviços que tenham sido prejudicados;

(v) Avaliação da necessidade de notificação de todas as partes internas e externas apropriadas (por exemplo, administrador fiduciário, clientes ou investidores afetados, segurança pública);

(vi) Avaliação da necessidade de publicação do fato ao mercado, nos termos da regulamentação vigente, a fim de garantir a ampla disseminação e tratamento equânime da informação, se privilegiada);

(vii) Determinação do responsável que arcará com as perdas decorrentes do incidente, a cargo do Comitê de Compliance, após a condução de investigação e uma avaliação completa das circunstâncias do incidente.

6. Arquivamento de Informações

De acordo com o disposto neste Manual, os Colaboradores deverão manter arquivada toda e qualquer informação, bem como documentos e extratos que venham a ser necessários para a efetivação satisfatória de possível auditoria interna e/ou externa ou investigação de órgãos regulatórios em torno de possíveis atuações da Gauss Capital, investimentos e/ou clientes suspeitos de corrupção e/ou lavagem de dinheiro (conforme política de lavagem de dinheiro da Gauss Capital), em conformidade com o inciso IV do Artigo 16 da Instrução CVM 558/15.

7. Propriedade Intelectual

A lei de propriedade intelectual dispõe claramente que toda invenção e modelo de utilidade pertencem exclusivamente ao empregador, neste caso a Gauss Capital, quando decorrerem de trabalho cuja execução se deu durante o período de vínculo do Colaborador com a Gauss Capital.

Desta forma, todos os documentos e arquivos, incluindo, sem limitação, aqueles produzidos, modificados, adaptados ou obtidos pelos Colaboradores, relacionados, direta ou indiretamente, com suas atividades profissionais junto à Gauss Capital, tais como minutas de contrato, memorandos, cartas, fac-símiles, apresentações a clientes, e-mails, correspondências eletrônicas, arquivos e sistemas computadorizados, planilhas, fórmulas, planos de ação, bem como modelos de avaliação, análise e gestão, em qualquer formato, são e permanecerão sendo propriedade exclusiva da Gauss Capital, razão pela qual o Colaborador compromete-se a não utilizar tais documentos, no presente ou no futuro, para quaisquer fins que não o desempenho de suas atividades na Gauss Capital, devendo todos os documentos permanecer em poder e sob a custódia da Gauss Capital, sendo vedado ao Colaborador, inclusive, disseminar e retransmitir tais documentos, bem como apropriar-se de quaisquer desses documentos e arquivos após seu desligamento da Gauss Capital, salvo se autorizado expressamente pelo Diretor de Risco e Compliance e ressalvado o disposto abaixo.

Caso um Colaborador, ao ser admitido, disponibilize à Gauss Capital documentos, planilhas, arquivos, fórmulas, modelos de avaliação, análise e gestão ou ferramentas similares para fins de desempenho de sua atividade profissional junto à Gauss Capital, o Colaborador deverá assinar declaração nos termos do Anexo I ao presente Manual, confirmando que: (i) a utilização ou disponibilização de tais documentos e arquivos não infringe quaisquer contratos, acordos ou compromissos de confidencialidade, bem como não viola quaisquer direitos de propriedade intelectual de terceiros; e (ii) quaisquer alterações, adaptações, atualizações ou modificações, de qualquer forma ou espécie, em tais documentos e arquivos, serão de propriedade exclusiva da Gauss Capital, sendo que o Colaborador não poderá apropriar-se ou fazer uso de tais documentos e arquivos alterados, adaptados, atualizados ou modificados após seu desligamento da Gauss Capital, exceto se aprovado expressamente pelo Diretor de Risco e Compliance.

Ademais, nenhum colaborador da Gauss Capital será remunerado além da remuneração previamente acordada, por qualquer trabalho que constitua invenção ou modelo de utilidade, quando no desenvolvimento de suas atividades na Gauss Capital.

8. Revisão da Política

O Diretor de Risco e Compliance deverá realizar uma revisão da Política de Segurança da Informação e Cibernética a cada 12 (doze) meses, no mínimo, para avaliar a eficácia da sua implantação, identificar novos riscos, ativos e processos e reavaliando os riscos residuais, incluindo no relatório anual de compliance eventuais deficiências encontradas.

A finalidade de tal revisão será assegurar que os dispositivos aqui previstos permaneçam consistentes com as operações comerciais da Gauss Capital e acontecimentos regulatórios relevantes.

ANEXO I

TERMO DE PROPRIEDADE INTELECTUAL

Por meio deste instrumento eu, _____, inscrito no CPF sob o nº _____ ("Colaborador"), DECLARO para os devidos fins:

(i) que a disponibilização pelo Colaborador à **GAUSS CAPITAL GESTORA DE RECURSOS LTDA**, inscrita no CNPJ/MF sob o nº 21.052.737/0001-28 ("GAUSS CAPITAL"), nesta data, dos documentos contidos no *pen drive* da marca _____, número de série _____ ("Documentos"), bem como sua futura utilização pela GAUSS CAPITAL, não infringe quaisquer contratos, acordos ou compromissos de confidencialidade que o Colaborador tenha firmado ou que seja de seu conhecimento, bem como não viola quaisquer direitos de propriedade intelectual de terceiros;
(ii) ciência e concordância de que quaisquer alterações, adaptações, atualizações ou modificações, de qualquer forma ou espécie, nos Documentos, serão de propriedade exclusiva da GAUSS CAPITAL, sendo que o Colaborador não poderá apropriar-se ou fazer uso de tais documentos e arquivos alterados, adaptados, atualizados ou modificados após seu desligamento da GAUSS CAPITAL, exceto se aprovado expressamente pela GAUSS CAPITAL.

Para os devidos fins, o Colaborador atesta que os Documentos foram duplicados no pen drive da marca _____, número de série _____, que ficará com a GAUSS CAPITAL e cujo conteúdo é idêntico ao *pen drive* disponibilizado pelo Colaborador.

Os *pen drives* fazem parte integrante do presente termo, para todos os fins e efeitos de direito. A lista de arquivos constantes dos *pen drives* se encontra no Apêndice ao presente termo.

_____, ___ de _____ de _____.

_____
Colaborador:
CPF: