

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA
LUMINUS CAPITAL MANAGEMENT LTDA.
("Sociedade" ou "Luminus Capital")

CAPÍTULO I
DO OBJETIVO

1.1. O presente instrumento tem como objetivo precípuo a definição de regras e princípios norteadores das condutas dos colaboradores da Sociedade que tenham acesso a informações relevantes sobre a Sociedade, seus negócios ou clientes, em especial no que se refere à segurança da informação e segurança cibernética.

1.2. Os colaboradores atestam a ciência e adesão acerca dos procedimentos definidos pela presente Política mediante assinatura de termo próprio, sendo submetidos anualmente ao Programa de Treinamento adotado pela Sociedade, a fim de que sejam orientados sobre as rotinas a serem observadas no desempenho dos processos descritos nesta Política.

1.3. A Sociedade coletará Termo de Confidencialidade de quaisquer terceiros contratados que tiverem acesso às informações confidenciais a respeito da Sociedade, seus colaboradores, fundos sob gestão e investidores, salvo se este compromisso já tiver sido firmado entre as partes mediante a assinatura do correspondente Contrato de Prestação de Serviços.

1.4. A fim de cumprir o seu objetivo, esta Política será revisada no mínimo a cada 2 (dois) anos, sendo mantido o controle de versões, e circulada aos colaboradores para conhecimento e assinatura do Termo de Adesão e Confidencialidade supramencionado sempre que alterado.

1.5. Em caso de dúvidas ou necessidade de aconselhamento, o colaborador deve buscar auxílio junto ao Diretor de Compliance da Sociedade, devendo as questões de segurança cibernética serem tratadas com a empresa de tecnologia da informação terceirizada responsável.

CAPÍTULO II
PROCEDIMENTOS DE SEGURANÇA DA INFORMAÇÃO

I. ACESSO RESTRITO

2.1.1. A troca de informações entre os colaboradores da Sociedade deve sempre pautar-se no conceito de que o receptor deve ser alguém que necessita receber tais informações para o desempenho de suas atividades e que não está sujeito a nenhuma barreira que impeça o recebimento daquela informação. Em caso de dúvida a área de compliance deve ser acionada previamente à revelação.



2.1.2. Os colaboradores da Sociedade que tiverem acesso aos sistemas de informação serão responsáveis por tomar as precauções necessárias de forma a impedir o acesso não autorizado aos sistemas, devendo salvaguardar as senhas e outros meios de acesso aos mesmos.

2.1.3. Os arquivos da Sociedade são armazenados em nuvem e gerenciados por empresas de primeira linha.

2.1.4. O acesso controlado às pastas e arquivos se dá mediante a outorga de senhas de acesso individuais e intransferíveis que permitem a identificação do seu usuário, afastando a utilização das informações ali contidas por pessoas não autorizadas.

2.1.5. Adicionalmente, todas as mensagens enviadas/recebidas dos computadores disponibilizados pela Sociedade permitem a identificação do seu remetente/receptor.

2.1.6. O armazenamento de informações protegidas em dispositivos portáteis deve restringir-se aqueles autorizados pelo Diretor de Compliance, e o *upload* dos arquivos para estes dispositivos dar-se-ão necessariamente sob supervisão do mesmo.

2.1.7. A outorga e cancelamento de senhas é de responsabilidade do TI, sempre mediante orientação do Diretor Compliance, a quem compete a verificação da estrutura de governança da Sociedade, a fim de evitar a transgressão de barreiras de informação e potenciais conflitos de interesse. Este procedimento deverá ser observado ainda na hipótese de mudança de atividade/área de um determinado profissional dentro da Sociedade.

2.1.8. As senhas de acesso possuem prazo de validade e requisitos mínimos de segurança, devendo ser desabilitadas após um número máximo de tentativas malsucedidas de acesso, sendo esta atividade registrada pelos controles de tecnologia da informação.

2.1.9. Após um tempo máximo de inatividade, os sistemas internos e dispositivos fornecidos pela Sociedade expiram, usando um protetor de tela protegido por senha que exija que a sessão somente possa ser reiniciada depois que o usuário tenha se autenticado novamente.

2.1.10. No caso do desligamento ou saída de algum colaborador, o acesso aos arquivos será automaticamente bloqueado e a respectiva senha revogada. Para sistemas externos, a Sociedade deverá submeter uma solicitação de revogação de acesso imediatamente e assegurar-se de que os acessos sejam revogados.



2.1.11. O controle do acesso a arquivos confidenciais em meio físico é garantido através da segregação física da equipe de gestão de recursos de terceiros, na medida em que a Sociedade desempenha única e exclusivamente esta atividade.

II. BACK-UP

2.2.1 Todos os documentos arquivados no servidor da Sociedade são objeto de back-up diário com controle das alterações promovidas nos arquivos, garantindo a segurança dos respectivos conteúdos e eventual responsabilização.

2.2.2. Os prestadores de serviço terceirizados armazenam versões anteriores de arquivos por até 7 dias, ou seja, se algum arquivo for apagado ou alterado de forma errônea, é possível recuperá-lo durante este período.

2.2.3. Além da segurança proporcionada pelo armazenamento na nuvem, diariamente, é efetuado back-up automático de todos os arquivos criados ou alterados ao longo do dia de trabalho através de software especializado. As cópias de back-up são armazenadas em locais externos em empresas terceirizadas especializadas, sendo possível o acesso e/ou recebimento destas mídias em caso de contingência, mediante solicitação à equipe de TI terceirizada. Adicionalmente, o Diretor de Compliance mantém em sua residência 2 back-ups físicos (atualizados mensalmente) destes arquivos.

III. Cópia de Arquivos e instalações

2.3.1. Todos os programas de computador utilizados pelos colaboradores devem ter sido previamente autorizados pelo responsável pela área de informática. Downloads de qualquer natureza podem ser realizados, desde que de forma justificada.

2.3.2. A cópia de arquivos e instalação de programas em computadores deverá respeitar os direitos de propriedade intelectual pertinentes, tais como licenças e patentes.

2.3.3. É terminantemente proibido que os Colaboradores façam cópias (físicas ou eletrônicas) ou imprimam os arquivos utilizados, gerados ou disponíveis na rede e circulem em ambientes externos com estes arquivos, salvo se em prol da execução e do desenvolvimento dos negócios e dos interesses da Sociedade. Nestes casos, o colaborador que estiver na posse e guarda do arquivo será o responsável direto por sua boa conservação, integridade e manutenção de sua confidencialidade.

2.3.4. Qualquer impressão de documentos deve ser imediatamente retirada da máquina impressora, pois pode conter informações restritas e confidenciais mesmo no ambiente interno da Sociedade. É vedada, ainda, a manutenção destes em mesas, máquinas de fax ou copadoras.



IV. Descarte de Informações

2.4.1. O descarte de informações confidenciais deve observar as seguintes diretrizes:

- (i) o conteúdo descartado deverá ser apagado e/ou as mídias devem ser destruídas, impossibilitando a sua recuperação, de modo que a informação não fique vulnerável a acesso não autorizado;
- (ii) os documentos físicos que contenham informação protegida devem ser triturados imediatamente após seu uso de maneira a evitar sua recuperação ou leitura;
- (iii) a eliminação ou a destruição final das mídias ou documentos, realizada por terceiros, deve ser documentada;
- (iv) dispositivos de memória e dispositivos de armazenamento (por exemplo laptops, dispositivos USB, discos rígidos portáteis, tablets, smartphones) desativados pela Sociedade devem ser apagados de modo que a informação protegida que neles havia seja irrecuperável.

V. Redundância

2.5.1. Além das cópias de segurança acima, outros recursos de TI são redundantes. Em caso de pane e indisponibilidade de acesso físico ao local de trabalho, a equipe-chave, previamente designada e treinada para tanto, poderá acessar as informações na nuvem de qualquer local.

2.5.2. No tocante ao acesso à internet, a Sociedade dispõe de duas conexões banda larga do ligadas simultaneamente pelo Firewall, que permite a automática comutação e a divisão do tráfego para o serviço secundário, sempre que houver interrupção do serviço principal.

2.5.3. Para garantir o funcionamento da rede e a integridade dos dados, mesmo na eventual interrupção do fornecimento de energia elétrica, todas as estações de trabalho e o servidor estão conectados a um equipamento do tipo *no-break*, que permite a continuidade do funcionamento da rede por tempo suficiente para que os usuários salvem seus arquivos.

CAPÍTULO III SUPORTE E MONITORAMENTO

3.1. Em caso de pane da rede ou em alguma estação de trabalho, o fato deverá ser imediatamente comunicado à área de TI, que assegurará o suporte interno ou providenciará que seja acionado o suporte externo necessário.



3.2. O sistema eletrônico utilizado pela Sociedade está sujeito à revisão e monitoramento a qualquer época sem aviso ou permissão, de forma a detectar qualquer irregularidade na transferência de informações, seja interna ou externamente.

3.3. Nesse sentido, tendo em vista que a utilização do e-mail se destina exclusivamente para fins profissionais, como ferramenta para o desempenho das atividades dos colaboradores, a Sociedade também poderá monitorar toda e qualquer troca, interna ou externa, de e-mails dos colaboradores.

3.4. Qualquer suspeita ou conhecimento de violação desta Política ou incidente de segurança da informação deve ser objeto de informação ao Compliance para que sejam tomadas as devidas providências com relação à apuração dos fatos, mitigação de eventuais riscos, implementação de procedimentos corretivos e responsabilização dos envolvidos.

3.5. Periodicamente e sem aviso prévio, poderão ser realizadas inspeções nos computadores para averiguação de downloads impróprios, não autorizados ou gravados em locais indevidos.

Tratamento de casos de vazamento de informações confidenciais

3.6. No caso de vazamento de informações confidenciais relacionadas aos clientes da Sociedade, ainda que oriundo de ação involuntária, o Diretor de Compliance notificará os interessados sobre o ocorrido.

3.7. Sem prejuízo, a Sociedade acionará o seu Plano de Recuperação visando a identificação da causa que ensejou o vazamento e responsabilização do causador. Ademais, será elaborado um Relatório acerca dos danos ocorridos, percentual das atividades afetadas, impactos financeiros, sugerindo ainda medidas a serem tomadas de modo a possibilitar que as atividades voltem a ser executadas normalmente.

3.8. Este Relatório será elaborado pelo Diretor de Compliance e será submetido à Diretoria da Sociedade que promoverá as iniciativas cabíveis para o retorno à normalidade com a maior brevidade possível.

Firewall

3.9. A Sociedade faz o uso da tecnologia de Firewall para proteger sua rede contra ameaças externas.

Rede Wireless

3.10. A Sociedade possui 2 (duas) redes WIFI distintas, uma para uso interno e outra para uso dos visitantes. Jamais deve ser divulgada a senha de acesso interno para os visitantes. Os visitantes devem sempre solicitar a senha de acesso para um colaborador da Sociedade.



3.11. A rede WIFI para visitantes é bloqueada para acessar recursos internos.

Testes de Segurança

3.12. São realizados os seguintes testes de segurança para monitoramento dos sistemas utilizados:

ROTINAS OPERACIONAIS	PERIODICIDADE
Varredura de antivírus	Tempo real
Controle de conteúdo de Internet pelo Firewall e Antivírus	Tempo real
Varredura de memória pelo Antivírus	Tempo real
Autenticação de rede	Tempo real
Back Up Servidor	Diário
Atualizações nas estações de trabalho	Mensal

CAPÍTULO IV IDENTIFICAÇÃO E AVALIAÇÃO DE RISCOS CIBERNÉTICOS

4.1. Considerando a atividade de gestão profissional de recursos de terceiros desempenhada pela Sociedade são essenciais todos os recursos tecnológicos necessários ao processo de análise, investimento e desinvestimento, tais como: (i) disponibilização das informações diárias sobre os fundos sob gestão; (ii) boletagem de operações; (iii) compra e venda de ativos para as carteiras sob gestão; (iv) conferência e liberação das carteiras diárias dos fundos sob gestão; e (v) acesso aos sistemas de informação.

4.2. Abaixo são descritos os riscos internos identificados e respectivas avaliações. Para tanto, considerou-se: (i) possíveis ameaças; (ii) grau de exposição dos ativos supramencionados às ameaças; (iii) impactos financeiros, operacionais e reputacionais; e (iv) a expectativa de que o evento de segurança se efetive:

Risco Interno	Avaliação Inicial
Não se aplica.	-

Risco Externo	Avaliação Inicial
Queda de energia elétrica	Os impactos seriam mínimos ou até inexistentes. Vide plano de contingência explanado na Política de Gestão de Riscos.
Queda do serviço do Servidor	
Queda dos links de internet	
Impedimento de acesso ao escritório	



CAPÍTULO V AÇÕES DE PROTEÇÃO E PREVENÇÃO AOS RISCOS CIBERNÉTICOS

5.1. Os planos de ação e prevenção descritos neste Capítulo tem por objetivo mitigar e minimizar a possibilidade de ocorrência de um ataque cibernético, na tentativa de evitar que os riscos identificados se concretizem.

5.2. Neste sentido, a Sociedade ratifica a adoção de controles de acesso físico e lógico implementados em linha com a Política de Segurança da Informação adotada. Tais controles visam a identificação, autenticação e autorização de acesso pelos usuários a sistemas ou ativos da Sociedade, evitando o acesso por terceiros não autorizados.

5.3. Isto posto, todos os colaboradores devem observar de forma estrita as rotinas relacionadas à definição de senhas de acesso aos sistemas e rede, bem como às barreiras da informação com relação a outras atividades desempenhadas pela Sociedade ou empresas do mesmo grupo econômico.

5.4. Os eventos de login e alteração de senhas são rastreáveis e auditáveis, sendo qualquer inconsistência ou inadequação com relação aos acessos recomendados pelo Diretor de Compliance reportados imediatamente. Especial atenção deverá ser envidada aos casos de desligamento ou gozo de férias de colaboradores.

5.5. São adotadas as seguintes medidas preventivas para cada risco identificado:

Risco Interno	Ação de Proteção/Prevenção
Exclusão acidental de arquivos do servidor	A empresa responsável realiza back-up diário dos arquivos do servidor e pode recuperar imediatamente (mediante solicitação) qualquer arquivo que venha a ser excluído.

Risco Externo	Ação de Proteção/Prevenção
Infecção dos equipamentos por vírus	Todos os e-mails e navegadores são equipados com anti-vírus para evitar qualquer infecção. Adicionalmente, a empresa de TI contratada pode acessar os equipamentos da Sociedade a qualquer momento para realizar qualquer reparo que se faça necessário.



5.6. Todos os novos equipamentos e sistema instalados na Sociedade devem contar com as configurações de proteção acima descritas, sendo realizado teste em ambientes de homologação e de prova antes do início da sua utilização. Sem prejuízo, são realizadas inspeções visando a verificação da atualização dos sistemas operacionais e softwares instalados nos computadores da Sociedade.

5.7. Todos os programas de computador utilizados pelos colaboradores devem ter sido previamente autorizados pelo responsável pela área de informática, sendo vedadas aplicações não autorizadas por meio de controles de execução de processos. Downloads de qualquer natureza podem ser realizados, desde que de forma justificada.

CAPÍTULO VI MECANISMOS DE SUPERVISÃO DA SEGURANÇA CIBERNÉTICA

6.1. São realizados os seguintes testes de verificação para fins de identificação de anomalias, detecção de ameaças, acessos, componentes ou dispositivos não autorizados:

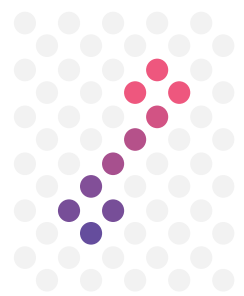
Rotina	Periodicidade
<i>Backup</i>	Diário
Teste de restauração de dados	Diário
Teste de invasão externa e phishing	Estabelecida pelo anti-vírus
Análise de Logs e trilhas de auditoria (Servidor)	Tempo-real

6.2. São mantidos inventários atualizados de hardware e softwares utilizados pela Sociedade. São realizadas verificações, a fim de identificar elementos estranhos à Sociedade, tais como computadores não autorizados ou softwares não licenciados.

6.3. Sempre que houver alteração relevante na estrutura tecnológica da Sociedade serão realizadas análises de vulnerabilidade.

CAPÍTULO VII RESPOSTAS A INCIDENTES CIBERNÉTICOS

7.1. A Sociedade adota os seguintes planos de ação de resposta a incidentes em função das ameaças identificadas:



Ameaça Interna	Plano de Ação
Qualquer ameaça interna.	Deve-se entrar em contato com a empresa de TI especializada em segurança cibernética.

Ameaça Externa	Plano de Ação
Qualquer ameaça externa.	Deve-se entrar em contato com a empresa de TI especializada em segurança cibernética.

7.2. Compete à Equipe de Compliance a comunicação da contingência aos demais colaboradores da Sociedade, orientando-os sobre a postura e providências cabíveis, de acordo com a natureza e severidade da contingência, em observância do Plano de Continuidade de Negócios.

7.3. Cabe à Equipe de Compliance desenvolver relatórios acerca dos danos ocorridos, percentual das atividades afetadas, impactos financeiros, sugerindo ainda medidas a serem tomadas de modo a possibilitar que as atividades voltem a ser executadas normalmente. Tais relatórios deverão ser submetidos à Diretoria da Sociedade que promoverá as iniciativas cabíveis para o retorno à normalidade com a maior brevidade possível.

7.4. Após o retorno à normalidade, na tentativa de evitar incidentes da mesma qualidade, a Sociedade estudará procedimentos preventivos a serem implementados e incluídos neste plano de continuidade de negócios.

CAPÍTULO VIII PROGRAMA DE TREINAMENTO

8.1. A Sociedade conta com um programa de treinamento dos colaboradores que tenham acesso a informações relevantes sobre a Sociedade, seus negócios ou investidores.

8.2. Os procedimentos e rotinas definidos na presente Política serão abordados em treinamento anual, coordenado pelo Diretor de Compliance ou terceiro contratado para esta finalidade, visando a sua disseminação entre a equipe da Sociedade.

8.3. Poderão ser promovidos treinamentos em periodicidade menor, visando a atualização e ampliação do conhecimento dos colaboradores, em especial em virtude de mudanças relevantes nos procedimentos e controles descritos nesta Política.

CAPÍTULO IX DISPOSIÇÕES GERAIS E ENFORCEMENT



9.1. Todos os documentos, relatórios e informações relevantes para os procedimentos e rotinas descritos nesta Política são arquivados em meio físico ou eletrônico na Sociedade, pelo prazo mínimo de 5 (cinco) anos.

9.2 O presente Instrumento prevalece sobre quaisquer entendimentos orais ou escritos anteriores, obrigando os colaboradores da Sociedade aos seus termos e condições.

9.3. A título de *enforcement*, vale notar que a não observância dos dispositivos da presente Política resultará em advertência, suspensão, demissão ou exclusão por justa causa, conforme a gravidade e a reincidência na violação, sem prejuízo das penalidades civis e criminais.