EXPRESSO
PLANEJAMENTO FINANCEIRO

AV. NIEMEYER, Nº 02 | SALA 207 | LEBLON
CEP 22450 220 | RIO DE JANEIRO | RJ
TEL 55 21 2249 4809 | FAX 55 21 2294 9890

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E SEGURANÇA CIBERNÉTICA

EXPRESSO PLANEJAMENTO GESTÃO DE RECURSOS LTDA.
("Sociedade")

Versão vigente: Fevereiro/2023

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, assim entendidos: seus (i) sócios; (ii) diretores; (iii) funcionários; (iv) estagiários ou (v) quaisquer pessoas que, em virtude de seus cargos, funções ou posições na Sociedade, 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 o responsável pela Tecnologia da Informação.

AV. NIEMEYER, Nº 02 | SALA 207 | LEBLON
CEP 22450 220 | RIO DE JANEIRO | RJ
TEL 55 21 2249 4809 | FAX 55 21 2294 9890

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. 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.

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

2.1.5. O armazenamento de informações protegidas em dispositivos portáteis deve restringir-se àqueles fornecidos pela Sociedade.

2.1.6. 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.

2.1.7. 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.

AV. NIEMEYER, Nº 02 | SALA 207 | LEBLON
CEP 22450 220 | RIO DE JANEIRO | RJ
TEL 55 21 2249 4809 | FAX 55 21 2294 9890

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

2.1.9. 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.

2.1.10. O controle do acesso a arquivos confidenciais em meio físico é garantido através da segregação física da equipe de gestão de recursos de terceiros.

II. Backup

2.2.1 Todos os documentos arquivados nos Servidores da Sociedade são objeto de backup diário em HD externo e no servidor com controle das alterações promovidas nos arquivos, garantindo a segurança dos respectivos conteúdos e eventual responsabilização.

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 copiadoras.

AV. NIEMEYER, Nº 02 | SALA 207 | LEBLON
CEP 22450 220 | RIO DE JANEIRO | RJ
TEL 55 21 2249 4809 | FAX 55 21 2294 9890

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 no HD externo ou nos e-mails que são armazenados na nuvem.

2.5.2. No tocante ao acesso à internet, a Sociedade dispõe de duas conexões banda larga, 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

AV. NIEMEYER, Nº 02 | SALA 207 | LEBLON
CEP 22450 220 | RIO DE JANEIRO | RJ
TEL 55 21 2249 4809 | FAX 55 21 2294 9890

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.

AV. NIEMEYER, Nº 02 | SALA 207 | LEBLON
CEP 22450 220 | RIO DE JANEIRO | RJ
TEL 55 21 2249 4809 | FAX 55 21 2294 9890

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 possuí 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 a recepcionista.

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
Monitoramento de Hosts e serviços	Tempo real
Autenticação de rede	Tempo real
Bloqueio de tela do Windows por Inatividade	A cada 15 min
Backup Firewall	A cada alteração
Verificar status dos logs do Backup	Mensal
Backup Diário	Diário
Backup Mensal	Mensal
Teste de restore do backup	Mensal
Reiniciar Servidores - Atualizações Microsoft	Semanal
Verificar status Nobreak CPD	Mensal
Atualizações Microsoft nas estações de trabalho	Semanal
Verificar Antivírus	Semanal

AV. NIEMEYER, Nº 02 | SALA 207 | LEBLON
CEP 22450 220 | RIO DE JANEIRO | RJ
TEL 55 21 2249 4809 | FAX 55 21 2294 9890

Varredura do HD local pelo Antivírus	Semanal
Shutdown programado nas estações de trabalho, caso estejam ligadas	Semanal
Troca da senha dos usuários	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) boletagem de operações; (ii) compra e venda de ativos para as carteiras sob gestão; (iii) conferência e liberação das carteiras diárias dos fundos sob gestão; e (iv) acesso aos sistemas de informação.

4.2. Diante da possibilidade de invasores utilizarem (i) *Malware*, (ii) Engenharia social; (iii) *Pharming*; (iv) *Phishing*; (v) *Vishing*; (vi) *Smishing*; (vii) Acesso pessoal; (viii) Ataques de DDos (distributed denial of services) e *botnets*; e (ix) Invasões (advanced persistent threats, a Sociedade adota ações de prevenção e proteção, nos termos do Capítulo seguinte.

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.

AV. NIEMEYER, Nº 02 | SALA 207 | LEBLON
CEP 22450 220 | RIO DE JANEIRO | RJ
TEL 55 21 2249 4809 | FAX 55 21 2294 9890

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 Externo	Ação de Proteção/Prevenção
Tentativa de invasão a rede interna	O Firewall instalado na rede analisa todo o tráfego de entrada na rede. Caso um dos acessos seja suspeito o próprio firewall de forma proativa realiza o bloqueio e alerta o TI local do acesso bloqueado.

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.

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
Backup	Diário
Teste de restauração de dados	Mensal
Teste de invasão externa e phishing	Semestral
Teste de resposta a incidentes com simulação de cenários	Semestral
Análise de Logs e trilhas de auditoria	Diário

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

AV. NIEMEYER, Nº 02 | SALA 207 | LEBLON
CEP 22450 220 | RIO DE JANEIRO | RJ
TEL 55 21 2249 4809 | FAX 55 21 2294 9890

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 /Externa	Severidade (Classificação)	Plano de Ação
Qualquer nível	Leve/Média/Grave	Contato com o a equipe de TI ou algum diretor da sociedade para analisar de forma detalhada a ameaça afim de aplicar as manobras necessárias.

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.

AV. NIEMEYER, Nº 02 | SALA 207 | LEBLON
CEP 22450 220 | RIO DE JANEIRO | RJ
TEL 55 21 2249 4809 | FAX 55 21 2294 9890

CAPÍTULO VIII
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.

9.4. A presente Política será revisada, no mínimo, a cada 2 (dois) anos, salvo se demandar ajustes em períodos menores.

9.5. A versão vigente desta Política encontra-se registrada na ANBIMA, sendo encaminhada nova versão sempre que alterada, no prazo máximo de 15 (quinze) dias contados da alteração.