



ASSUNTO:

**POLÍTICA INTERNA**  
**SEGURANÇA CIBERNÉTICA**

CÓDIGO: PI - 13

REVISÃO: 1.0

DATA: DEZ/20

## 1. OBJETIVO

Este documento (“Política de Segurança Cibernética”) tem como objetivo estabelecer os princípios, conceitos, valores e práticas que devem ser adotados pelos colaboradores, prestadores de serviços e parceiros da Corretora, também bem como de determinar regras, exposição e ferramentas de segurança a serem analisadas para uma melhor utilização e funcionamento dos sistemas de segurança cibernética.

Ademais, essa política tem a função de auxiliar a empresa e seus colaboradores a continuarem em correspondência conformidade com as regras, aos padrões éticos e profissionais.

Com as diretrizes, essa política busca reduzir os riscos de acordo com o caráter, complexidade e risco das atividades desempenhadas pela Novinvest, além disso, tem a finalidade de que cada Colaborador provenha o mais alto nível de padrão ético no desempenho de suas atividades.

## 2. ABRANGÊNCIA

Esta Política abrange todos os colaboradores da Novinvest.

## 3. DOCUMENTOS VINCULADOS

- i. Resolução (CMN) nº 4658 de 26/04/2018,
- ii. ICVM 612 de 21/08/2019,
- iii. Políticas Internas.

## 4. CONTROLE DE REVISÕES

VERSÃO	DATA	ELABORADO POR:	CONFERIDO POR:	DESCRIÇÃO DAS ALTERAÇÕES
0	ABR/19	Marcos Rocha	Suêmi Ranieri	Política de Segurança Cibernética – substituição total
01	DEZ/20	Ediley Bispo	Suêmi Ranieri	Política nova

<b>ELABORADO POR:</b> <i>Compliance</i>	<b>REVISADO POR:</b> Jurídico	Página 1 de 10
--	----------------------------------	----------------



ASSUNTO:

**POLÍTICA INTERNA**

**SEGURANÇA CIBERNÉTICA**

CÓDIGO:

PI - 13

REVISÃO:

1.0

DATA:

DEZ/20

## 5. DIRETRIZES

### 5.1 PRINCÍPIOS DA SEGURANÇA DA INFORMAÇÃO

Os princípios básicos da segurança da informação são: confidencialidade, integridade e disponibilidade das informações. Outras características são: irrefutabilidade, 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.

**Confidencialidade:** Proteção da informação compartilhada contra acessos não autorizados. Ameaça à segurança acontece quando há uma quebra de sigilo de uma determinada informação, permitindo que sejam expostas voluntária ou involuntariamente dados restritos e que deveriam ser acessíveis apenas por um determinado grupo de usuários.

**Integridade:** Garantia da veracidade da informação, pois a mesma não deve ser alterada enquanto está sendo transferida ou armazenada. Ameaça à segurança acontece quando uma determinada informação fica exposta ao manuseio por uma pessoa não autorizada, que efetua alterações não aprovadas e sem o controle do proprietário (corporativo ou privado) da informação.

**Disponibilidade:** Prevenção contra as interrupções das operações da empresa como um todo. Os métodos para garantir a disponibilidade incluem um controle físico e técnico das funções dos sistemas de dados, assim como a proteção dos arquivos, seu correto armazenamento e a realização de cópias de segurança. As ameaças à segurança acontecem quando a informação deixa de estar acessível para quem necessita dela.

A ciência pelos Colaboradores das práticas, rotinas e procedimentos previstos nesta Política não os desobriga de ter conhecimento e de observar os conteúdos previstos nas demais políticas internas da Corretora.

<b>ELABORADO POR:</b> <i>Compliance</i>	<b>REVISADO POR:</b> Jurídico	Página 2 de 10
--	----------------------------------	----------------



ASSUNTO:

## POLÍTICA INTERNA

### SEGURANÇA CIBERNÉTICA

CÓDIGO:

PI - 13

REVISÃO:

1.0

DATA:

DEZ/20

Os Colaboradores que desejarem maiores informações sobre as demais políticas, ou que tenham qualquer dúvida a respeito do conteúdo desta, deverão contatar a equipe de Compliance ou a área de TI.

#### 5.2 AÇÕES PARA IMPLEMENTAR AS DIRETRIZES DA POLÍTICA DE SEGURANÇA CIBERNÉTICA

A Corretora estabeleceu um conjunto de medidas buscando mitigar os riscos identificados, ou seja, buscar impedir previamente a ocorrência de um ataque cibernético, incluindo a programação e implementação de controles, na forma abaixo:

- Cada Colaborador é responsável por manter o controle sobre a segurança das informações armazenadas ou disponibilizadas nos equipamentos sob sua responsabilidade.

#### 5.3 PROCEDIMENTOS E OS CONTROLES ADOTADOS PARA REDUZIR A VULNERABILIDADE

Com a contratação de prestador de serviços para a segurança cibernética, buscamos a segurança da informação, com aplicações que permitem maior flexibilidade na gestão das políticas de segurança, facilitando a construção das regras e tornando-as mais legíveis:

- Com controle e bloqueio de redes sociais e pornografia, controle do tráfego de internet, de maneira a proteger a rede corporativa limitando o usuário a navegar apenas em páginas de interesse da corporação.
  1. O firewall por aplicação, além de identificar comportamentos padrões, identifica não somente nos cabeçalhos, mas também na área de dados dos pacotes.
  2. Proteção de navegação, não permite o acesso de site que espalhe trojans, spyware ou qualquer outro tipo de software malicioso, impedirá que se conecte e seja infectado.

<b>ELABORADO POR:</b> <i>Compliance</i>	<b>REVISADO POR:</b> Jurídico	Página 3 de 10
--	----------------------------------	----------------



ASSUNTO:

## POLÍTICA INTERNA

### SEGURANÇA CIBERNÉTICA

CÓDIGO:

PI - 13

REVISÃO:

1.0

DATA:

DEZ/20

3. Bloqueio a sites perigosos e acessos fraudulentos para evitar phishing e downloads por acidente de malwares.
4. Protetor de arquivo, uma camada de proteção que verifica todos os arquivos baixados.
5. Bloqueio por comportamento, detecta novas ameaças que não são conhecidas pelo comportamento comum de ataques.
6. Anti-Ransomware, monitoramento comportamental personalizado impede o ransomware antes que ele possa criptografar dados.
7. VPN utilizando protocolo OPENVPN no caso de acesso externo podendo autenticar-se através de um usuário que foi adicionado ao UTM ou autenticação no AD (Active Directory). No caso de acesso à Internet o UTM poderá autenticar o usuário no AD ou usuário local (adicionado ao UTM) VPN com escolha do protocolo de criptografia.
8. Firewall NG/UTM permite inúmeros mecanismos tais como: VLAN, segmentação de redes diferentes para cada interface de rede, etc..
9. Backup do UTM no Cloud do backup automático
10. Varreduras - Por meio do log do Firewall, Webfilter, VPN, e demais serviços
11. Através do Mail Security podemos Monitorar o Vazamento de Senha, Disponibilidade de Servidores POP|IMAP|SMTP, Monitor pro-ativo de Blacklist, Filtro de entrada Anti-Spam, Quarentena de e-mails, Relatórios gerenciais, Regras gerais e individuais.

A Corretora mantém conexões ativas redundantes e em alta velocidade através da compactação, criptografia dos pacotes e protocolos L2TP, IPSec ou OpenVPN. Ligação VPN.

A prevenção e a detecção de intrusão: IPS (Intrusion Prevention system) : Identifica tentativas de ataques e toma ações automáticas para evitar incidentes de segurança;

A proteção contra softwares maliciosas através do Kaspersky

<b>ELABORADO POR:</b> <i>Compliance</i>	<b>REVISADO POR:</b> Jurídico	Página 4 de 10
--	----------------------------------	----------------



ASSUNTO:

## POLÍTICA INTERNA

### SEGURANÇA CIBERNÉTICA

CÓDIGO:

PI - 13

REVISÃO:

1.0

DATA:

DEZ/20

O estabelecimento de mecanismos de rastreabilidade: Por meio do log do Firewall, Webfilter, VPN, e demais serviços

Os controles de acesso e de segmentação de redes de computadores: Firewall NG/UTM permite inúmeros mecanismos tais como: VLAN, segmentação de redes diferentes para cada interface de rede, rede de produção, homologação, contingência, workstation.

Manutenção de cópias de segurança: Backup do UTM no Cloud através do backup automático e backup diário conforme as rotinas de backup adotadas.

- **ACESSO CONTROLADO AO DATACENTER**

A linha de Firewall contratada possui a função IPS, responsável por detectar arquivos intrusos na rede. Os malwares e outros vírus, tentam invadir a rede sozinhos ou por intermédio de usuários involuntários. Neste caso a função IPS monitora os acessos e detecta a tentativa de invasão. Os malwares são bloqueados automaticamente e os usuários infectados são desinfetados antes de entrar na rede.

IPS – Intrusion Prevention system: Identifica tentativas de ataques e toma ações automáticas para evitar incidentes de segurança;

#### 5.4 DIRETRIZES DE SEGURANÇA DA INFORMAÇÃO

Adoção de Comportamento Seguro: Independentemente do meio e/ou da forma em que se encontrem, as Informações Sigilosas podem ser encontradas na rede e fazem parte do ambiente de trabalho de todos os Colaboradores de forma segregada conforme regras aplicadas no Active Directory. É fundamental para a proteção delas que os Colaboradores adotem comportamento seguro e consistente, com destaque para os seguintes itens:

- a) Os Colaboradores devem assumir atitude proativa e engajada no que diz respeito à proteção das Informações Sigilosas;

<b>ELABORADO POR:</b> <i>Compliance</i>	<b>REVISADO POR:</b> Jurídico	Página 5 de 10
--	----------------------------------	----------------



ASSUNTO:

## POLÍTICA INTERNA

### SEGURANÇA CIBERNÉTICA

CÓDIGO:	PI - 13
REVISÃO:	1.0
DATA:	DEZ/20

- b) Os Colaboradores devem compreender as ameaças externas que podem afetar a segurança das informações sigilosas, tais como vírus de computador, interceptação de mensagens eletrônicas, grampos telefônicos, etc., bem como fraudes destinadas a roubar senhas de acesso aos sistemas de tecnologia da informação em uso e aos servidores;
- c) Todo tipo de acesso aos dados e informações, em especial as Informações sigilosas, que não forem expressamente autorizadas, é proibido;
- d) Assuntos relacionados ao desempenho de atividades e funções da Corretora não devem ser discutidos em ambientes públicos ou em áreas expostas (e.g. meios de transporte, locais públicos, encontros sociais);
- e) As senhas de acesso do Colaborador aos sistemas são pessoais e intransferíveis, não podendo ser compartilhadas, divulgadas a terceiros (inclusive a outros Colaboradores), anotadas em papel, ou em sistema visível ou de acesso não protegido;
- f) Os Colaboradores devem bloquear seus computadores sempre que se ausentarem de suas estações de trabalho;
- g) Somente softwares homologados e previamente aprovados podem ser instalados e usados nas estações de trabalho, o que deve ser feito com exclusividade pela área de TI da Corretora;
- h) Arquivos eletrônicos de origem desconhecida não devem ser abertos e/ou executados nos computadores;
- i) O acesso remoto à rede, às Informações Sigilosas e sistemas, somente será permitido mediante autorização do usuário que se torna responsável pelas ações tomadas a partir do momento da aprovação e autorização do acesso. O

<b>ELABORADO POR:</b> <i>Compliance</i>	<b>REVISADO POR:</b> Jurídico	Página 6 de 10
--	----------------------------------	----------------



ASSUNTO:

**POLÍTICA INTERNA**  
**SEGURANÇA CIBERNÉTICA**

CÓDIGO:	PI - 13
REVISÃO:	1.0
DATA:	DEZ/20

colaborador que aprovou o acesso será corresponsável pela segurança do acesso remoto aos sistemas e Informações Sigilosas;

- j) O Colaborador deve evitar realizar acesso remoto à rede a partir de um dispositivo público, e, caso o faça, deverá limpar o cache e deletar todos os arquivos temporários;
- k) Documentos impressos e arquivos contendo Informações Sigilosas devem ser adequadamente armazenados e protegidos, sendo vedada a retirada da sede da Gestora sem a autorização prévia do superior hierárquico do Colaborador. É terminantemente proibido o envio de mensagens e arquivos anexos que possam causar constrangimento à terceiros, bem como com conteúdo político ou outro que possa colocar a empresa em risco. A Novinvest se reserva o direito de monitorar o uso dos dados, informações, serviços, sistemas e demais recursos de tecnologia disponibilizados aos seus Colaboradores, e que os registros e o conteúdo dos arquivos assim obtidos poderão ser utilizados para detecção de violações aos documentos internos da corretora, e, conforme o caso, servir como evidência em processos administrativos, arbitrais ou judiciais.

Uma vez que colaboradores, fornecedores, prestadores de serviços e parceiros, também podem representar uma fonte significativa de riscos de segurança cibernética, a Novinvest ministrará periodicamente palestras educacionais a seus Colaboradores, em parceria com a empresa contratada, a fim de conscientizar e disseminar a cultura de segurança da informação e segurança cibernética, sendo aplicado uma avaliação a todos presentes.

Antes da contratação de todo e qualquer serviço que pode de forma direta ou indireta envolver processamento, armazenamento e computação em nuvem, deve previamente ter aval da área jurídica da Novinvest, para que possa consultar e comunicar banco central.

- A computação em nuvem pode ser considerada como uma forma de contratação de serviço de terceiros e, assim como as demais contratações de fornecedores,

<b>ELABORADO POR:</b> <i>Compliance</i>	<b>REVISADO POR:</b> Jurídico	Página 7 de 10
--	----------------------------------	----------------



ASSUNTO:

## POLÍTICA INTERNA

### SEGURANÇA CIBERNÉTICA

CÓDIGO:

PI - 13

REVISÃO:

1.0

DATA:

DEZ/20

prestadores de serviços e parceiros, envolve determinados riscos que devem ser levados em conta pela corretora, demandando certos cuidados proporcionais a esta identificação de ameaças.

#### 5.5 ÁREA RESPONSÁVEL PELO REGISTRO E CONTROLE DOS EFEITOS DOS INCIDENTES

A equipe de TI, em conjunto com o Diretor de Compliance, sendo a principal responsável dentro da Corretora para tratar e responder questões de segurança cibernética (“Responsável pela Segurança Cibernética”), bem como por implementar as regras e normas aqui estabelecidas e a sua revisão.

Na ocorrência de qualquer incidente envolvendo risco cibernético, todo e qualquer Colaborador que perceba ou desconfie de tal incidente deverá imediatamente informar o Responsável por Segurança Cibernética.

#### 5.6 PROCEDIMENTO EM CASO DE INCIDENTES

Consideramos como incidente relevante, manuseio de dados ou informações sensíveis à pessoa externa não autorizada. Uma vez que o Responsável pela Segurança Cibernética tenha sido acionado devido a um potencial incidente, este deverá observar os procedimentos abaixo:

- **AVALIAÇÃO INICIAL**

Nessa etapa inicial, aspectos e decisões fundamentais deverão ser analisadas pelo Responsável pela Segurança Cibernética, em conjunto com a Diretoria e tomadas após o incidente. O foco da reunião deverá compreender uma análise do que aconteceu, motivos e consequências imediatas, bem como a gravidade da situação, devendo decidir pela formalização ou não do incidente.

- **INCIDENTE CARACTERIZADO**

<b>ELABORADO POR:</b> <i>Compliance</i>	<b>REVISADO POR:</b> Jurídico	Página 8 de 10
--	----------------------------------	----------------





ASSUNTO:

## POLÍTICA INTERNA

### SEGURANÇA CIBERNÉTICA

CÓDIGO:

PI - 13

REVISÃO:

1.0

DATA:

DEZ/20

Se for caracterizado um incidente, medidas imediatas deverão ser tomadas, que poderão abranger se será registrado um boletim de ocorrência ou queixa crime, informar ao Compliance que determinará qual órgão deverá ser informado sobre o ocorrido, envolver o setor jurídico, comunicar interna ou externamente, em especial ao investidor que tenha sido afetado e verificar se houve prejuízo para a Corretora ou investidor específico.

Além disso, a Diretoria, em conjunto com a área de TI, Compliance, Jurídico e eventual consultor, deverá definir os passos a serem tomados sob o aspecto de *Cibersegurança*, tais como iniciar a redundância de TI, redirecionar as linhas de telefone para os celulares, instruir o provedor de telefonia a desviar linhas de dados/e-mail, entre outros.

- **RECUPERAÇÃO**

Essa fase começa após o incidente inicial ter sido contornado, já tendo sido a redundância de TI acionada.

Será realizado um call ou uma reunião presencial, conforme o caso, em periodicidade a ser definida, para acompanhamento pela Diretoria, para estabelecer as medidas a serem tomadas, responsabilidades e prazos. Também deverá ser avaliado o impacto do incidente nos diversos riscos e, caso necessário, tomar as devidas ações, tais como manifestação pública na mídia, enquanto que a Diretoria verificará se todas as informações necessárias estão seguras e a área de gestão definirá se decisões de investimento são requeridas.

Quaisquer dados faltantes ou corrompidos, ou problemas identificados por Colaboradores da Corretora, devem ser comunicados à Diretoria, a área de TI, Compliance e Jurídico. Fornecedores, prestadores de serviços e parceiros relevantes deverão ser mantidos atualizados.

<b>ELABORADO POR:</b> <i>Compliance</i>	<b>REVISADO POR:</b> Jurídico	Página 9 de 10
--	----------------------------------	----------------



ASSUNTO:

## POLÍTICA INTERNA

### SEGURANÇA CIBERNÉTICA

CÓDIGO:	PI - 13
REVISÃO:	1.0
DATA:	DEZ/20

- **RETOMADA**

Tal fase refere-se ao período de transição do retorno ao modo normal de operação e pode incluir a análise de projetos, reconstrução de eventuais sistemas e eventuais mudanças e medidas de prevenção. A ocorrência deverá registrar o histórico do ocorrido, causa, com o maior nível de detalhes possível, consultando todos os envolvidos em todos os níveis.

#### 6. APROVAÇÃO E VIGÊNCIA

Esta Política foi aprovada pela Diretoria Colegiada, em ordem alfabética, a via original está disponível na área de Compliance e estará em vigor na data da sua publicação.

<b>ELABORADO POR:</b> <i>Compliance</i>	<b>REVISADO POR:</b> Jurídico	Página 10 de 10
--	----------------------------------	-----------------

## ATA DE REUNIÃO de 29/06/2021

**ASSUNTO:** Atualização de Políticas – Cibernética e Segurança da Informação

1. DATA/HORA E LOCAL – Aos 29 (vinte e nove) dias do mês de junho de 2021, às 12h00min (doze horas), na sede da sociedade, na Rua Boa Vista, nº 63, 10º Andar, CEP nº 01014-001, Centro, São Paulo, SP, devidamente inscrita no CNPJ/MF sob o nº. 43.060.029/0001-71.
2. PRESENÇA – José Oswaldo Morales Júnior / Máuricio Leal da Silva / Silvio Alexandre Rocha da Silva / Ediley Alberto Bispo.



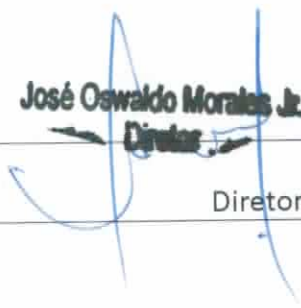

A reunião teve início com a apresentação dos documentos abaixo, com todas as explicações e alterações necessárias para o atendimento da legislação vigente.

Foram repassados cada item das Políticas, a saber:

- Política de Segurança Cibernética PI13 – v1,
- Política de Segurança da Informação PI12 – v1.

Todos os diretores concordaram com as explicações, com os assuntos nas Políticas e a metodologia aplicada para evidenciar os controles para mitigação aos riscos.

3. ENCERRAMENTO E APROVAÇÃO DA ATA - Os trabalhos foram encerrados e aprovados por todos os diretores (assinaram os documentos). Os documentos podem ser divulgados na rede interna.

 Ediley Alberto Bispo Compliance	 Silvio Alexandre Diretor Operações	 José Oswaldo Morales Jr. Diretor	 Maurício Leal Diretor Administrativo
Diretores			