- POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA -

VERSÃO	DATA	RESPONSÁVEL
1	Outubro de 2019	Diretora de Gestão de Riscos e Compliance.

1. ESCOPO

O objetivo desta Política é delinear os processos existentes na **BRESCO GESTÃO E CONSULTORIA LTDA.** ("Bresco"), globalmente e no Brasil, relacionados à segurança da informação e cibernética, em atendimento à regulação e autorregulação aplicável, principalmente os artigos 13, 14, 16 e 17 do Código de Regulação e Melhores Práticas para Administração de Recursos de Terceiros da ANBIMA.

2. INTRODUÇÃO

A Bresco por si ou por suas entidades afiliadas, atua como gestora de fundos de investimentos, em especial fundos de investimentos imobiliários na aquisição, no desenvolvimento e na administração de imóveis através de operações de *built to suit, sale-leaseback*, aquisição e desenvolvimento de terrenos e propriedades para locação e/ou venda, entre outros.

Os imóveis geridos pela Bresco integram na presente data, o portfolio dos fundos Bresco Logística Fundo de Investimento Imobiliário ("Bresco Logística"), Bresco Growth Fundo de Investimento Imobiliário ("Bresco Growth") e Bresco International Fund SPC ("Bresco International" e, em conjunto com Bresco Logística e Bresco Growth, "Fundos").

Sem prejuízo, a Bresco poderá vir a gerir outros fundos de investimentos com estratégias diversificadas de investimento em ativos imobiliários ou diferentes públicos-alvo. Para todos os fins, outros fundos de investimentos que venham a ser geridos pela Bresco estão incluídos na definição de "Fundos" no âmbito desta política para todos os fins.

2.1. INFORMAÇÃO RELEVANTE

Entende-se por "Informação Relevante" toda e qualquer informação, conteúdo ou dado que tenha valor para a Bresco, seus funcionários, clientes e investidores. Além do que está armazenado nos computadores, o termo Informação Relevante engloba também as informações disponíveis em relatórios, documentos, arquivos físicos, ou até mesmo quando repassada através de conversas dentro ou fora da empresa.

Portanto, quando nos referimos a "segurança da informação", falamos de proteções voltadas às informações impressas, verbais e sistêmicas, bem como nos controles de acesso, vigilância, contingência de desastres naturais, contratações, cláusulas e demais questões que, juntas, formam uma proteção adequada para qualquer empresa.

Esta Política constitui 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. Ela também define as atribuições de cada um dos profissionais em relação à segurança

dos recursos com os quais trabalham, além de prever o que pode ser feito e o que será considerado inaceitável com relação ao assunto.

2.2. PRINCÍPIOS DE SEGURANÇA DA INFORMAÇÃO

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

- 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 expostos, voluntária ou involuntariamente, dados restritos e que deveriam ser acessíveis apenas a um determinado grupo de usuários.

- Integridade: Garantia da veracidade da informação, pois a mesma não deve ser alterada enquanto está sendo transferida ou armazenada. Ameaças à segurança acontecem 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.

Além disso, como regra geral aplicável a todas as unidades operacionais da Bresco, o acesso dos usuários às informações é restrito e controlado, significando que só as pessoas que devem ter acesso a uma determinada informação terão, de fato, esse acesso.

3. O PLANO DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA DA BRESCO

A Bresco possui políticas, processos e controles destinados à proteção e segurança das Informações Relevantes ("Plano"), com o fim de:

- Identificar e mensurar riscos previsíveis relacionados à segurança, confidencialidade e/ou integridade de todos os documentos contendo Informações Relevantes da Bresco, bem como avaliar e, se for o caso, melhorar a eficácia das proteções já em vigor destinadas à prevenção ou mitigação de tais riscos;

- Prevenir que ex-funcionários da Bresco tenham acesso a documentos contendo Informações Relevantes;

- Supervisionar os prestadores de serviços da Bresco que tenham acesso a Informações Relevantes; e

- Restringir acesso a dados e documentos contendo Informações Relevantes e assegurar o seu correto armazenamento e transferência.

3.1. RESPONSÁVEIS PELO PLANO DE SEGURANÇA DA INFORMAÇÃO

O Plano é operado e mantido pela Diretora de Gestão de Riscos e *Compliance* da Bresco.

Adicionalmente à Diretora de Gestão de Riscos e *Compliance* e da Área de Risco e *Compliance*, o Plano será gerido e supervisionado pelo time de TI e pelo Diretor de Gestão de Recursos.

3.2. PROTEÇÕES DO PLANO

No escopo do Plano, foram desenvolvidas proteções administrativas, técnicas e físicas para gerir os riscos relacionados à segurança da informação, incluindo os cibernéticos. Essas proteções foram implementadas com base no modelo de negócios da Bresco e estão alinhadas com a regulação aplicável e melhores práticas de segurança da informação.

a) Proteções Administrativas

As proteções administrativas focam em aspectos de governança, políticas, procedimentos e manutenção do Plano. As seguintes medidas foram implementadas nesse sentido.

Governança e Modelo de Operação

Conforme se depreende do tópico anterior, um modelo de segurança cibernética da informação foi estabelecido, implementado e integrado na Bresco como um todo, incluindo: (i) a indicação do responsável geral pela manutenção do Plano, e (ii) o envolvimento, supervisão e apoio de diversos grupos de trabalho dedicados a esse fim, conforme indicados no tópico "*Responsáveis pelo Plano de Segurança da Informação*".

Diretora de Gestão de Risco e *Compliance*

A Diretora de Gestão de Risco e *Compliance* tem responsabilidade geral pela manutenção do Plano, o qual foi desenvolvido para assegurar que os controles destinados a proteger as Informações Relevantes estão em plena operação e alinhados ao modelo de negócios da Bresco e demais requisitos regulatórios aplicáveis.

O Plano poderá ser atualizado periodicamente como resultado de:

- processos de avaliação de risco;
- mudanças substanciais nos negócios da Bresco;
- novas tendências ou instruções da indústria e da regulação; e
- ameaças cibernéticas emergentes.

Atualizações Regulatórias

O departamento jurídico da Bresco monitora periodicamente as atualizações regulatórias relacionadas à privacidade e segurança da informação que possam ser relevantes e aplicáveis ao Plano, trabalhando com a Diretora de Risco e *Compliance* na implementação de eventuais alterações necessárias às políticas, regras e controles internos da Bresco.

Supervisão de Prestadores de Serviços

A Bresco adota procedimentos para selecionar, reter e supervisionar prestadores de serviços terceirizados, com o fim de avaliar se estes possuem, mantêm e aplicam ritos adequados para preservação da privacidade e segurança das informações por eles recebidas no curso da prestação de serviços. Alguns desses procedimentos da Bresco incluem, mas não se limitam a: (i) revisar e fazer cumprir obrigações contratuais relacionadas à segurança das informações compartilhadas com os prestadores de serviço terceirizados; (ii) a realização de diligências (*due diligence*) para avaliação de riscos da segurança da informação relativamente a determinados prestadores de serviços, de forma a confirmar que medidas apropriadas de proteção à informação estão sendo adotadas por eles; e (iii) quando tecnicamente viável, monitorar o acesso do prestador de serviços a Informações Relevantes e sistemas da Bresco.

Treinamento e Conscientização

Conforme mencionado acima, a Bresco adota políticas e procedimentos especialmente desenhados para a proteção de Informações Relevantes. Os empregados recebem treinamentos periódicos relacionados à proteção de dados e informações, bem como sobre confidencialidade e segurança das Informações Relevantes. Tais treinamentos são consistentes com as leis aplicáveis e razoavelmente desenhados para agregar um nível adequado de conhecimento e conscientização aos nossos empregados. Adicionalmente, boletins sobre segurança da informação são enviados periodicamente a todos os empregados da Bresco.

b) Proteções Técnicas (*cybersecurity*)

As proteções técnicas são especialmente desenhadas para proteger as Informações Relevantes de ataques cibernéticos (*cyber-attacks*) e outras ameaças eletrônicas. Com relação a esse tópico, as seguintes medidas foram implementadas no âmbito do Plano:

Continuidade de Negócios

O plano de continuidade de negócios e de recuperação de desastres da Bresco assegura que informações vitais da operação do grupo sejam protegidas e recuperadas dentro dos prazos desejados no evento de um *cyber-attack* ou de outro evento que afete a continuidade dos negócios.

Identificação de Usuários e Gestão ao Acesso às Informações

A Bresco estabeleceu controles para identificação dos usuários e acesso às informações para ajudar na proteção das unidades operacionais do grupo contra acessos não autorizados a Informações Relevantes. Esses controles incluem, entre outros itens:

- Conceder aos empregados contas individuais e ID's e requerer que os empregados elaborem senhas de alta complexidade para dificultar o acesso a seus *logs*;
- Exige-se que os empregados atualizem suas senhas periodicamente; e
- Bloqueio ao acesso de usuários em caso de erros sucessivos na digitação de senhas no momento do *login*.

A Bresco restringe o acesso a Informações Relevantes apenas a empregados que realmente precisem acessar tais dados para desempenhar seu trabalho (*need-to-know*). Além disso, o acesso eletrônico dos trabalhadores aos sistemas da Bresco é imediatamente interrompido em caso de desligamento, incluindo a desativação de senhas e de nomes de usuário.

A Bresco possui também um processo para administração de mudanças no quadro funcional com o fim de atualizar o acesso dos empregados a Informações Relevantes, conforme necessário, em razão de alteração das funções e/ou responsabilidades de determinados empregados. Revisões periódicas aos acessos dos usuários são realizadas de forma a assegurar o seu devido funcionamento.

Gestão de Informações sobre Ativos

As Informações Relevantes da Bresco são geridas de acordo com controles de acesso definidos com base na necessidade de acesso, prioridades e esperado grau de proteção a tais dados. Por exemplo, o acesso à rede da Bresco de local remoto requer múltipla autenticação pelo usuário (*multi-factor authentication – MFA*) e o uso de dispositivos removíveis (e.g., *pendrives,* CD, etc.) em computadores de empregados da Bresco é restrito. Se tecnicamente viável, todos os documentos e arquivos contendo Informações Relevantes que irão ser transferidos por redes públicas, assim como todos os dados contendo Informações Relevantes transmitidos via *wireless* e todas as Informações Relevantes armazenadas em *laptops* ou outros dispositivos portáteis, serão criptografados. Além disso, a Bresco trabalha com prestadores de serviços, parceiros de negócio

e outras partes externas com o fim de proteger Informações Relevantes transmitidas via correio eletrônico ou por outros mecanismos de transmissão.

Plano de Resposta a Incidentes

A Diretora de Gestão de Risco e *Compliance*, em conjunto com o departamento jurídico, revisará e apropriadamente responderá a relatórios sobre incidentes que venham a reportar um risco de furto de identidade de usuário ou a efetiva violação material de Informações Relevantes, de acordo com as políticas e procedimentos aplicáveis. As respostas apropriadas a estes incidentes incluem, mas não se limitam a:

- O monitoramento de processos de negócios e contas de usuários;

- Adotar procedimentos razoáveis de modo a assegurar que o incidente seja isolado e não sistêmico;

- Reforçar processos de negócio e controles internos de modo a prevenir a recorrência do incidente;

- Adotar medidas razoáveis de modo a assegurar que qualquer parte que inadvertidamente recebeu Informações Relevantes não tenha usado tal Informação Relevante em seu favor, e que os arquivos associados contendo as Informações Relevantes foram devolvidos, deletados ou destruídos por tal pessoa;

- Alterar senhas, códigos de segurança ou outros dispositivos de segurança que permitam acesso a Informações Relevantes;

- Contatar o dono da Informação Relevante, agência reguladora, autoridade governamental competente ou especialistas forenses, para que sejam adotadas as medidas apropriadas, em conformidade à regulamentação aplicável; e

- Coordenar o início do plano de continuidade de negócios, se aplicável.

Gestão de Ameaças e Vulnerabilidade

A Área de Gestão de Risco e *Compliance* em conjunto com a equipe de TI continuamente monitora e procura administrar ameaças contra a segurança das Informações Relevantes. O programa de gestão de ameaças da Bresco inclui, mas não está limitado a: (i) a administração de vulnerabilidades; e (ii) o monitoramento de ameaças. A administração de vulnerabilidades inclui a realização periódica da avaliação da vulnerabilidade dos sistemas e a realização de testes de penetração, bem como a avaliação da infraestrutura associada à Informação Relevante de forma a verificar a resiliência dos sistemas da Bresco. Sistemas cruciais aos negócios da Bresco estarão

mais sujeitos a testes de vulnerabilidade do que outros sistemas de caráter mais operacional. Já o monitoramento de ameaças inclui o recebimento de atualizações sobre ameaças cibernéticas emergentes fornecidas por prestadores de serviços *experts* em inteligência da segurança da informação, especialmente contratados para esse fim.

c) Proteções Físicas

As proteções físicas se destinam a salvaguardar informações cruciais sobre ativos e Informações Relevantes de ameaças físicas e ambientais. As seguintes medidas são aplicáveis:

Segurança Física e Ambiental

A Bresco estabeleceu controles para proteção das informações cruciais sobre seus ativos (e.g., computadores, servidores, etc.) contra ameaças relacionadas ao ambiente físico onde estão localizados os servidores, bem como contra acessos não autorizados a tais ambientes. Para esse fim, o acesso físico às instalações da Bresco é sempre controlado. Empregados e visitantes são solicitados a usarem identificações individuais para entrar nas áreas de trabalho. O *hardware* utilizado na infraestrutura da Bresco, é hábil a garantir a resistência dos arquivos e dados armazenados contra riscos ambientais, destacando-se a implementação de controles como a presença de geradores de energia, sistemas de resfriamento, conectividade, *no-breaks* e o uso de sistemas e infraestrutura de emergência, em caso de desastres ou outros incidentes ambientais, para a manutenção dos sistemas da Bresco por tempo suficiente até que os serviços possam ser completamente restaurados.

Segurança dos Equipamentos de Acesso a Empregados

A Bresco bloqueia imediatamente o acesso físico a arquivos e documentos em relação a empregados desligados. Empregados desligados são também solicitados a devolver todos os documentos contendo Informações Relevantes (incluindo documentos físicos ou eletrônicos), bem como chaves, IDs, plaquetas de identificação ou outros itens que lhes garantam acesso às áreas internas da Bresco ou a documentos que contenham Informações Relevantes.

3.3. Procedimentos e Regras Aplicáveis às Informações de Clientes

a) Não Divulgação de Informações de Clientes

A Bresco tem o compromisso firme de proteger a privacidade das informações pessoais não divulgadas ao público dos seus clientes conforme definido em seus procedimentos ("Informações de Clientes") e possui procedimentos para salvaguardar registros e informações dos clientes. Informações de Clientes podem ser fornecidas a terceiros que não são coligadas da Bresco apenas nas circunstâncias descritas a seguir, salvo outras restrições impostas por regulamentos e leis locais:

- Por solicitação ou com consentimento do cliente;
- A terceiros conforme necessário para viabilizar as atividades da Bresco; e
- A reguladores e outros, conforme exigido ou permitido por lei.

Às vezes, as Informações de Clientes podem ser revisadas pelos prestadores de serviços externos da Bresco (por ex.: contadores, advogados, consultores, administradores, etc.). Esses prestadores de serviços são cientificados da natureza confidencial das informações e devem manter a confidencialidade das Informações de Clientes.

É vedado aos funcionários, durante a vigência do contrato de trabalho ou após o desligamento da Bresco, divulgar as Informações de Clientes a qualquer pessoa ou entidade fora da Bresco, inclusive familiares, exceto nas circunstâncias descritas acima.

Um funcionário tem a permissão de divulgar Informações de Clientes somente para outros funcionários ou agentes que precisam ter acesso a tais informações para entregar nossos serviços ao investidor.

A regra de confidencialidade aplica-se às informações em todos e quaisquer formatos, sejam elas obtidas de uma conversa, documentos escritos ou por outro meio. A conscientização sobre segurança da informação implica também que nenhuma informação da Bresco deverá ser deixada em local não seguro. Os funcionários são instruídos a tomar todas as medidas necessárias para proteger e preservar os documentos ou qualquer objeto de valor que esteja em seu poder contra o uso indevido, questionamento impróprio ou exposição indesejada.

b) Salvaguarda e Disponibilização de Informações de Clientes

A Bresco restringe o acesso às Informações de Clientes àqueles funcionários que precisam das informações para fornecer serviços a nossos clientes.

Qualquer funcionário com acesso autorizado às Informações de Clientes deve guardar tais informações em compartimentos ou receptáculos seguros no encerramento do expediente, todos os dias. Todos os arquivos de computador ou eletrônicos que contenham tais informações devem estar protegidos contra acesso não autorizado. Quaisquer conversas envolvendo informações pessoais não divulgadas ao público, quando apropriado, devem ser conduzidas por funcionários em particular, e deve-se tomar cuidado para evitar que essas conversas sejam ouvidas por acaso ou interceptadas por pessoas autorizadas.

Qualquer funcionário autorizado a ter a posse de "informações de relatórios de clientes para um propósito de negócio deve tomar medidas razoáveis para proteger-se contra o acesso não autorizado ou o uso das informações em relação à sua disponibilização.

c) Correio eletrônico (e-mail) e outras comunicações comerciais eletrônicas

A política da Bresco estabelece que e-mail, mensagens instantâneas e outras comunicações eletrônicas são tratadas como comunicações por escrito e que tais comunicações devem sempre ser de natureza profissional. Nossa política abrange as comunicações eletrônicas da Bresco, enviadas para ou recebidas de nossos clientes e investidores, e inclui comunicações por e-mail dentro da Bresco.

"Comunicações comerciais eletrônicas" são comunicações de um funcionário da Bresco a um terceiro na condução do negócio da Bresco por meios eletrônicos, tais como e-mail ou mensagens instantâneas ("MI"). Os funcionários da Bresco podem conduzir o negócio através dos seguintes formatos eletrônicos aprovados: (i) e-mail do Outlook da Bresco; (ii) MI da Bresco (apenas para uso interno); e (iii) excepcionalmente, mediante anuência da Diretora de Risco e *Compliance*, mensagem de texto e aplicativo *WhatsApp*. O negócio da Bresco não pode ser conduzido através de mensagens de texto (exceto, na hipótese mencionada acima, quando houver aprovação da Diretora de Risco e *Compliance*), sites de redes sociais (por ex.: Facebook, Twitter, LinkedIn, etc.), ou contas de e-mail pessoal (por ex.: Yahoo!, Gmail, etc.). As comunicações comerciais eletrônicas que possam ser consideradas materiais de propaganda requerem aprovação da Área de Gestão de Risco e *Compliance* antes da distribuição.

É importante salientar que as comunicações comerciais eletrônicas e quaisquer comunicações eletrônicas, inclusive comunicações pessoais, feitas em sistemas da Bresco (por ex.: e-mail do Outlook e MI da Bresco), são de propriedade da Bresco. Essas comunicações podem ser revisadas, buscadas ou apresentadas em litígios, investigações regulatórias ou iniciativas internas. Por conseguinte, os funcionários não devem ter nenhuma expectativa de privacidade nessas comunicações e devem fazer comunicações pessoais o mínimo possível.

A Bresco também introduzirá o registro de chamadas telefônicas internas e externas e, sempre que apropriado, cuidará dos seguintes temas: (i) consentimento das partes para a gravação de uma chamada telefônica; (ii) solicitação e aprovação para uso de recursos de gravação de voz; (iii) acesso a chamada telefônica gravada; (iv) armazenamento, arquivamento e transferência de chamadas telefônicas gravadas. Qualquer exceção aos temas mencionados deve ser informada imediatamente à Diretora de Gestão de Risco e *Compliance* e por este ser aprovada.

A Bresco deve providenciar registros ordenados de sua organização comercial e interna, inclusive todos os serviços e transações realizadas por ela. Ainda, a Bresco deve reter registros em um meio que permita que as informações sejam armazenadas de maneira acessível para consulta futura por qualquer autoridade competente e para satisfazer as seguintes condições:

- qualquer autoridade competente deve ser capaz de acessar as informações prontamente e reconstituir todos os estágios importantes do processamento de cada transação;

- deve ser possível verificar facilmente quaisquer correções ou outras alterações, e o conteúdo dos registros antes de tais correções e alterações; e
- não deve ser possível, de outro modo, manipular ou modificar os registros.

Além disso, a fim de proteger informações valiosas da Bresco e evitar sua remoção das instalações da Bresco, os funcionários estão expressamente proibidos de usar mídias removíveis (por ex.: CDs, DVDs, USB e similares) ou links de comunicação (por ex.: cabo, rádio, infravermelho e etc.) em qualquer computador pertencente à Bresco, salvo com autorização prévia por escrito da Diretora de Gestão de Risco e *Compliance*.

4. Monitoramento

Os tópicos a seguir descrevem as rotinas de monitoramento periódicas destinadas a manter e, conforme necessário, reforçar o Plano.

Avaliação de Riscos

Avaliações periódicas de riscos à segurança cibernética e das informações são conduzidas para mensurar adequadamente os riscos atuais. Tais procedimentos facilitam a identificação e avaliação de potenciais e previsíveis riscos à segurança, confidencialidade e/ou integridade das Informações Relevantes da BRESCO, bem como a mensuração e melhoramento, quando necessário, da eficácia das medidas de proteção atualmente adotadas para mitigar tais riscos. Esses procedimentos de avaliação mensuram riscos em diversas áreas da Bresco, incluindo, mas não se limitando, a segurança da área de tecnologia da informação e rede corporativa. Os resultados das avaliações de risco são discutidos pelos órgãos internos adequados dentro da governança corporativa da Bresco, de forma a contribuir com a estruturação de adequados procedimentos de resposta a tais riscos e quais atividades mitigadoras devem ser adotadas no futuro para o grupo como um todo ou para aquela área específica.

Monitoramento Contínuo e Revisão Anual do Plano

O Plano é monitorado de forma contínua para assegurar seu correto funcionamento com vistas à proteção das Informações Relevantes, incluindo a prevenção a acessos não autorizados ou uso não autorizado de Informações Relevantes, além da identificação da necessidade de medidas para reforçar a eficácia ou contundência do Plano, conforme necessário. Adicionalmente, o escopo do Plano será revisado pelo uma vez ao ano, ou com maior frequência, se necessário, em razão de mudanças significativas ao modelo de negócios ou alterações regulatórias.

Reportes de Violação ou Vulnerabilidades à Segurança

Se algum empregado souber ou suspeitar de uma fragilidade à segurança da informação, acessos não autorizados ou uso não autorizado de Informações Relevantes, ou qualquer violação a esta Política, tal empregado deverá reportar diretamente à Área de Risco e *Compliance* por e-mail.

5. Medidas Disciplinares

O não cumprimento das políticas e procedimentos aqui previstos pode resultar em medidas disciplinares, as quais podem incluir demissão e, se aplicável, comunicação às autoridades regulatórias competentes. Qualquer uma das pessoas supervisionadas também pode responder pessoalmente por qualquer ato ilegal ou ilegítimo cometido durante o período em que for funcionário da Bresco. Essa responsabilidade pode sujeitar a pessoa supervisionada às penalidades civis, criminais ou regulatórias. O monitoramento das políticas e procedimentos aqui estabelecidos e a aplicação das sanções aplicáveis em caso de violação de tais políticas e procedimentos serão realizados primariamente pela Diretora de Gestão de Risco e *Compliance*.

6. Revisão da Política

Esta Política poderá ser revisada anualmente ou a qualquer tempo, conforme item "4", acima, ou, no mínimo, a cada 24 (vinte e quatro) meses, em conformidade ao Código de Regulação e Melhores Práticas para Administração de Recursos de Terceiros da ANBIMA.

* * *