POLÍTICA DE SEGURANÇA E SIGILO DAS INFORMAÇÕES

Rua Wisard 273, Sala 6 | Vila Madalena, São Paulo – SP | CEP 05434-080

Controle de Versões

Versão	Data	Elaborado/Modificado Por	Descrição
1ª	Setembro/2023	Compliance	Versão Original
2ª	Dezembro/2023	Compliance	Versão atual

Sumário

1. Objetivo

A Política de Segurança e Sigilo das Informações ("Política") da PRX Capital Ltda., ("PRX Capital ou Gestora"), denominada neste documento "PRX Capital", visa preservar a confidencialidade, integridade e disponibilidade das informações no desempenho de suas atividades, descrevendo a conduta adequada para o seu manuseio, controle, proteção e descarte.

2. Regulamentação Aplicável

- Resolução CVM nº 21/21;
- Código ANBIMA de Administração e Gestão de Recursos de Terceiros;
- ANBIMA Regras e Procedimentos de Deveres Básicos; e
- Guia Anbima de Cibersegurança.

3. Abrangência

São abrangidos por esta política todos os Colaboradores que possuam acesso às dependências e/ou que tenham acesso a qualquer tipo de ativo de informação que pertença, ou que estejam sob a responsabilidade da PRX Capital.

4. Divulgação e Vigência

A Política de Segurança e Sigilo das Informações, será apresentada aos Colaboradores, com o propósito de desenvolver e manter uma efetiva conscientização de segurança, assim como promover o seu fiel cumprimento. A presente Política será divulgada por intermédio de mensagem eletrônica (e-mail), bem como disponibilizada em um diretório interno de acesso a todos os colaboradores.

Adicionalmente a PRX Capital irá disponibilizar a presente política no SSM ANBIMA e, caso seja atualizado, estes devem ser disponibilizados em até 30 (trinta) dias corridos da alteração/atualização

A presente Política entra em vigor na data de sua publicação e deverá ser revisto anualmente e atualizado pela Diretoria de Compliance, Riscoe e PLD serão utilizadas como base para sua atualização as legislações, instruções normativas e regulamentações vigentes na data da sua revisão.

5. Responsabilidades

A PRX Capital se utiliza de um profissional de TI, responsável por administrar a área de Tecnologia da Informação – TI e executar as atividades nas funções fundamentais e rotinas da área, é de responsabilidade da Diretoria de Compliance, Risco e PLD o gerenciamento e controle de qualidade do serviço de TI.

6. Ativos da Informação

A PRX Capital considera como ativos de informação todas as informações, disponíveis em qualquer meio, utilizadas ou manipuladas nas operações da gestora, bem como todos os sistemas, equipamentos e instalações onde estas informações são manuseadas ou armazenadas.

As informações podem ser apresentadas nas mais distintas formas escritas, faladas, transmitidas, digitadas, armazenadas ou processadas em qualquer equipamento, papel, telefone, programa de computador, base de dados ou outro meio existente. Seja qual for o estado ou o meio do qual a informação seja apresentada ou compartilhada, ela deverá estar sempre protegida adequadamente, de acordo com as normas definidas nesta Política.

Para que não haja dúvidas, a PRX Capital define como ativos de informação os seguintes itens:

(i) As informações criadas, processadas, acessadas, manuseadas ou armazenadas em qualquer meio ou sistema de informação da PRX Capital;

(ii) Os computadores, equipamentos, softwares, banco de dados, redes de comunicações e serviços de tecnologia utilizados pela gestora em suas operações, ou qualquer outro recurso, informático ou não, que seja utilizado nas atividades da gestora onde haja manipulação ou armazenamento de informações;

(iii) As instalações em que estão localizados os equipamentos, sistemas, documentos ou informações da PRX Capital;

(iv) Processos e controles internos que sejam parte da rotina das áreas de negócio da PRX Capital; e

(v) Governança da Gestão de Risco quanto às ameaças e planos de ação, de contingência e de continuidade de negócios.

7. Segurança da Informação

A Segurança da Informação nada mais é que 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. Define as atribuições de cada um dos profissionais em relação à segurança dos recursos com os quais trabalham, além disso, deve prever o que pode ser feito e o que será considerado inaceitável.

Entende-se por informação todo e qualquer conteúdo ou dado que tenha valor para a organização ou pessoa. Além do que está armazenado nos computadores, a informação também está impressa em relatórios, documentos, arquivos físicos, ou até mesmo repassada através de conversas nos ambientes interno e externo. Por isso, todo cuidado é pouco na hora de imprimir relatórios, jogar papéis no lixo, deixar documentos em cima da mesa, conversar em locais públicos ou com pessoas estranhas ao nosso meio.

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

Dessa forma, os princípios de segurança da informação, cujo objetivos constituem a preservação da propriedade da informação, notadamente sua confidencialidade, integridade e disponibilidade, permitindo o uso e compartilhamento de forma controlada, bem como o monitoramento e tratamento de incidentes provenientes de ataques cibernéticos.

Assim, a PRX Capital preserva suas informações quanto a:

- Confidencialidade: Garantir que as informações sejam acessadas apenas por pessoas autorizadas;
- Integridade: Garantir que as informações, tanto em sistemas quanto em bancos de dados, estejam em um formato verdadeiro e correto para seus propósitos originais;
- Disponibilidade: Garantir que as informações e os recursos estejam disponíveis para aqueles que precisam delas quando necessário;
- Acesso Controlado: O acesso dos usuários à informação é restrito e controlado, significando que só as pessoas que devem ter acesso a uma determinada informação, tenham esse acesso. Ameaça à segurança acontece há descuido ou possível quebra da confidencialidade das senhas de acesso à rede;
- Finalidade: independentemente da forma apresentada ou do meio pelo qual é compartilhada ou armazenada, a informação deve ser utilizada unicamente para a finalidade para a qual foi autorizada;
- Necessidade: garantir que cada Colaborador tenha acesso exclusivamente às informações necessárias ao desempenho de suas atribuições.

8. Gerenciamento De Segurança Cibernética

A Segurança Cibernética constitui-se da preservação das propriedades da informação, notadamente sua confidencialidade, integridade e disponibilidade, permitindo o uso e o compartilhamento da informação de forma controlada, bem como do monitoramento e tratamento de incidentes provenientes de ataques cibernéticos. A segurança cibernética é o conjunto de tecnologias, processos e práticas projetados para proteger a rede, os computadores, os sistemas e os dados de ataques ou acessos não autorizados.

O risco de ataque cibernético ameaça os princípios da segurança das informações, tais como confidencialidade, integridade e disponibilidade.

A segurança cibernética deverá garantir:

- a segurança dos sistemas e dos bancos de dados;
- o gerenciamento das pessoas autorizadas;
- a segurança dos sistemas e informações que estão na nuvem;
- a segurança para todos os dispositivos/equipamentos;
- o planejamento da continuidade do negócio; e
- o treinamento constante do usuário final, com o objetivo de minimizar a vulnerabilidade da organização.

No que se refere especificamente à segurança cibernética, a PRX Capital identificou as seguintes principais ameaças, nos termos inclusive do 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 na informação acima, a PRX 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 restabelecimento da segurança devida.

9. Riscos da Informação

No âmbito de suas atividades, a PRX 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 PRX 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 PRX Capital e as tecnologias desenvolvidas internamente e por terceiros, suas ameaças possíveis e sua vulnerabilidade;
- Processos e Controles: processos e controles internos que sejam parte da rotina das áreas de negócio da PRX Capital;
- Governança da Gestão de Risco: a eficácia da gestão de risco pela PRX Capital quanto às ameaças e planos de ação, de contingência e de continuidade de negócios; e
- Tratamento de Dados Pessoais: De forma geral, sempre que houver a coleta de informações relacionadas à pessoa física, essas informações serão consideradas Dados Pessoais para fins da legislação de proteção de dados, a LGPD, a Lei 13.709/18 e redações dadas pela Lei nº 13.853/19.

10. Classificação da Informação

Para que se possam prevenir eventuais ataques cibernéticos e vazamento de informações, primeiro deve-se definir quais informações são as de maior sensibilidade para Gestora, assim

como aquelas que teriam o maior impacto financeiro, operacional e reputacional para PRX Capital, em caso de incidente de segurança.

Deste modo, a PRX Capital de Recursos segrega as informações geradas pela Gestora, aperfeiçoando a implementação de processos e o devido manuseio, armazenamento, transporte e descarte destas informações.

Todas as informações seguem uma classificação de segurança, de maneira a serem adequadamente protegidas quanto ao seu acesso e uso, sendo que, para aquelas consideradas de alta criticidade, são necessárias medidas especiais de tratamento. A classificação das informações deverá seguir a seguinte ordem:

(i) Pública: É uma informação da PRX Capital ou de seus clientes com linguagem e formato dedicado à divulgação ao público em geral, sendo seu caráter informativo, comercial ou promocional. É destinada ao público externo ou ocorre devido ao cumprimento de legislação vigente que exija publicidade.

(ii) Interna: É uma informação da PRX Capital que ela não tem interesse em divulgar, onde o acesso por parte de indivíduos externos à empresa deve ser evitado. Caso esta informação seja acessada indevidamente, poderá causar danos à imagem da organização, porém, não com a mesma magnitude de uma informação confidencial. Pode ser acessada sem restrições por todos os empregados e prestadores de serviços da PRX Capital .

(iii) Confidencial: É uma informação crítica para os negócios da PRX Capital ou de seus clientes. A divulgação não autorizada dessa informação pode causar impactos de ordem financeira, de imagem, operacional ou, ainda, sanções administrativas, civis e criminais à PRX Capital ou aos seus clientes. É sempre restrita a um grupo específico de pessoas, podendo ser este composto por empregados, clientes e/ou fornecedores.

(iv) Restrita: É toda informação que pode ser acessada somente por usuários da PRX Capital explicitamente indicado pelo nome ou por área a que pertence. A divulgação não autorizada dessa informação pode causar sérios danos ao negócio e/ou comprometer a estratégia de negócio da organização.

As informações digitais da PRX Capital, são classificadas de acordo com os seguintes critérios:

- Quaisquer informações e/ou dados que a PRX Capital teve acesso ou conhecimento por ser de domínio público (“Informação Pública”);
- Quaisquer informações e/ou dados que não estejam sujeitas a compromissos ou acordos de confidencialidade;
- Quaisquer informações e/ou dados que tenham a obrigatoriedade de divulgação por lei ou autoridade competente;
- Quaisquer informações que venham a ter a obrigatoriedade de divulgação por lei ou autoridade competente, mas o termo legal ainda não foi iniciado ou findado (Ex. Data de Divulgação);
- Todas as Informações Confidenciais, a saber: o know-how, técnicas, cópias, diagramas, modelos, amostras, programas de computador, informações técnicas, financeiras, estatísticas, logísticas ou relacionadas às estratégias de investimento ou comerciais,

incluindo saldos, extratos e posições de clientes e/ou dos fundos geridos pela PRX Capital;

- operações estruturadas, demais operações e seus respectivos valores, analisadas ou realizadas para os fundos de investimento e carteiras geridas pela PRX Capital ; e
- estruturas, planos de ação, relação de clientes, contrapartes comerciais, fornecedores e prestadores de serviços, bem como informações estratégicas, mercadológicas ou de qualquer natureza relativas às atividades da PRX Capital e/ou de seus sócios e clientes.

A partir da definição acima, a PRX Capital se empenhará para manter controles, conforme o nível de criticidade das informações e dados, sendo certo de que a prioridade será escalonada na seguinte ordem de relevância.

Nenhuma informação da PRX Capital classificada como confidencial pode ou deve ser discutida em locais inapropriados, como lugares públicos ou fechados, na presença de terceiros ou pessoas não diretamente relacionadas ao assunto, ou adiante daqueles sem autorização para conhecimento dessas informações. Todos os Colaboradores estão proibidos de fazer transitar, por qualquer meio, qualquer informação que não seja de domínio público, fora dos procedimentos estabelecidos por esta política e em normas específicas da PRX Capital para trânsito de informações.

Qualquer informação sobre a PRX Capital , ou de qualquer natureza relativa às atividades da PRX Capital e aos sócios e clientes, obtida em decorrência do desempenho das atividades normais dos Colaboradores, só poderá ser fornecida ao público, mídia ou a demais órgãos caso autorizado pelo Compliance, apontado nos termos do Código de Ética e Conduta da PRX Capital.

11. Propriedade dos Recursos De TI

Todos os recursos computacionais e de sistemas disponibilizados para os Colaboradores podem ser de propriedade da PRX Capital ou pessoal do Colaborador (Bring Your Own Device - BYOD). Essa definição é salvo expressa permissão da Diretoria de Compliance, Risco e PLD.

É importante notar que os ativos da PRX Capital podem estar localizados interna ou externamente ao ambiente da gestora, sendo sua ferramenta homologada pela Diretoria. Essa ferramenta contribui para a PRX Capital no requisito, segurança da informação e para a melhor a segurança cibernética, reduzir os custos e capacitar os colaboradores para trabalhar de praticamente qualquer lugar. A PRX Capital realiza o gerenciamento da: gestão de conteúdos, gestão documental, criação acessos, permissões colaborativos todas armazenadas em um diretório seguro para armazenar, organizar, compartilhar e acessar informações.

Ademais, a PRX Capital utiliza um serviço e ferramenta de armazenamento em nuvem, com ele é possível armazenar e hospedar qualquer arquivo, usando uma individual de cada colaborador. Também é possível definir arquivos públicos, somente em grupos restritos, usuários definidos ou privados.

12. Regras Gerais e Diretrizes de Segurança e de Uso de Tecnologia

São regras gerais para uso de tecnologia na PRX Capital:

- Quando o usuário se comunicar através de recursos de tecnologia da PRX Capital a linguagem falada ou escrita deve ser profissional, de modo que não comprometa a imagem da gestora;
- Os conteúdos acessados e transmitidos através dos recursos de tecnologia da PRX Capital devem ser legais, de acordo com o Código de Ética e Conduta, e devem contribuir para as atividades profissionais do usuário.
- O uso dos recursos de tecnologia da PRX Capital pode ser examinado, auditado ou verificado pelo TI, mediante autorização expressa da Diretoria, sempre respeitando a legislação vigente;
- Cada usuário é responsável pelo uso dos recursos que lhe foram fisicamente entregues, e estão sob sua custódia, garantindo a conservação, guarda e legalidade dos programas (softwares) instalados;
- Os recursos de tecnologia da PRX Capital, disponibilizados para os usuários, não podem ser repassados para outra pessoa interna ou externa à organização;
- Ao identificar qualquer irregularidade no recurso de tecnologia o usuário deve comunicar imediatamente à área de Riscos e Controles Internos;
- Os programas aplicativos, programas básicos (sistema operacional e ferramentas) e componentes físicos são implantados e configurados pela área de infraestrutura da PRX Capital;
- É desabilitado aos usuários implantar novos programas ou alterar configurações sem a permissão formalizada da área de infraestrutura da PRX Capital;
- É desabilitado ao usuário implantar ou alterar componentes físicos no computador;
- É implantada a proteção de tela no computador e/ou proteção de ausência (após um tempo de inatividade, o computador bloqueia o sistema, exigindo senha para ser usado novamente);
- É implantado o “log-off” automático por inatividade durante o período de 24 horas.

Programas Ilegais

É terminantemente proibido o uso de programas ilegais (sem licenciamento) e homologação da PRX Capital. Os usuários não podem, em hipótese alguma, instalar qualquer "software" (programa) nos equipamentos da gestora sem autorização prévia e expressa.

Uso de Senhas

As senhas são únicas, pessoais e intrasferíveis e tornam o portador da senha responsável por todas as ações praticadas, inclusive se utilizadas por terceiros. O compartilhamento de senhas, em quaisquer hipóteses, é expressamente proibido. As senhas deverão ser trocadas, conforme aviso fornecido pelo sistema/software utilizado. Como melhores práticas poderão ser trocadas semestralmente.

Firewall, Software, Varreduras

A PRX Capital mantém 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 gestora (por exemplo, vírus, worms, spyware). Essa proteção é realizada pela Antivirus homologado. Serão conduzidas varreduras diárias e mensais para detectar e limpar qualquer programa que venha a obter acesso a um dispositivo na rede interna da Gestora. A PRX Capital utiliza um plano de manutenção projetado para guardar os seus dispositivos e softwares contra vulnerabilidades com o uso de varreduras e patches.

Compartilhamento de Dados e Processamento, Armazenamento de Dados, Backup e Computação em Nuvem

Não é permitido o compartilhamento de pastas nos computadores e desktops da PRX Capital sem autorização prévia. Todos os dados deverão ser armazenados em rede/nuvem, e a autorização para acessá-los deverá ser fornecida pelo Compliance. O Backup é realizado em nuvem OneDrive é realizado diariamente de forma automática.

Utilização de Internet e Correio Eletrônico

A utilização da internet por nossos colaboradores deve ter como finalidade profissional.

Nossos colaboradores têm uma conta de e-mail em seu nome sendo esta, de sua inteira responsabilidade, devendo ser utilizada de acordo com as normas de conduta ética e de segurança do PRX Capital, sendo sua utilização estritamente profissional.

Destruição de Documentos

Descarte de Informações Confidenciais em meio digital deve ser feito de forma a impossibilitar sua recuperação. O descarte de documentos físicos que contenham informações confidenciais ou de suas cópias deverá ser realizado imediatamente após seu uso de maneira a evitar sua recuperação ou leitura.

Monitoramento

O Compliance implantará as medidas necessárias para realizar o monitoramento, bem como para estabelecer as permissões de acesso aos documentos e arquivos da Gestora. Nesse sentido, o monitoramento poderá ser realizado pelo Compliance. Todos os Colaboradores devem ter ciência de que o uso do e-mail, chats e informações corporativas estão sujeitas à monitoramento, sem frequência determinada ou aviso prévio.

Controle de Acesso

O acesso de pessoas estranhas à Gestora a áreas restritas somente é permitido com a autorização expressa de Colaboradores autorizados pelos administradores da PRX Capital.

Tendo em vista que a utilização de computadores, telefones, internet, e-mail e demais aparelhos

se destina exclusivamente para fins profissionais, sendo permitido o seu uso para fins pessoais de forma moderada, como ferramenta para o desempenho das atividades dos Colaboradores, a Gestora monitora a utilização de tais meios.

Home Office e/ou Acesso Remoto

A PRX Capital poderá adotar o home office e/ou acesso remoto como uma modalidade de trabalho. O Colaborador deverá observar o disposto estabelecido nesta Política, bem como a conduta ética prevista no Código de Ética e Conduta.

Antivírus

Recomendamos que o colaborador mantenha uma solução de antivírus atualizada e instalada no computador. O colaborador não pode em hipótese alguma, desabilitar o programa antivírus instalado nas estações de trabalho.

A PRX Capital mantém 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 gestora (por exemplo, vírus, worms, spyware). Serão conduzidas varreduras mensais para detectar e limpar qualquer programa que venha a obter acesso a um dispositivo na rede da PRX Capital.

Segurança Cloud ou de Segurança em Nuvem

Segurança em nuvem da PRX Capital é a ação de garantir que todos os dados e serviços que residem em uma nuvem sejam protegidos de ataques ou violações de disponibilidade, integridade e confidencialidade. As informações da Gestora são atualmente objeto de backup diário com o uso de computação na nuvem.

Programa de Gerenciamento de Incidentes TI

De acordo com o ITIL, uma biblioteca de boas práticas em gerenciamento de serviços de TI (ITSM), um incidente é a interrupção não planejada de um serviço de TI ou a redução da qualidade do serviço prestado.

O Programa de Gerenciamento de Incidentes da PRX Capital tem o objetivo de retomar um serviço o mais breve possível, causando o mínimo de danos ao negócio, de forma a mantê-lo no nível correntemente praticado por suas áreas de frente. Referido programa será composto pelas seguintes etapas:

- Identificação de Incidentes: o reconhecimento de incidentes da PRX Capital dar-se-á por meio de por sistemas de monitoramento internos, e pelos próprios usuários e clientes que se comunicarão com a Diretoria de Compliance, Risco e PLD por telefone ou e-mail.
- Registro de Incidentes: A ferramenta de controle de incidentes adotada pela PRX Capital será uma planilha para fins de registro dos mesmos e de suas respectivas soluções, de modo a estabelecer uma base de dados para correções e prevenções futuras.

- Categorização de Incidentes: a Diretoria de Compliance, Risco e PLD classificará o chamado recebido por (a) tipo: (1) trata-se de um incidente ou uma requisição; e (2) consiste em um chamado de hardware ou software?; e (b) a qual serviço do catálogo o incidente estará relacionado?
- Priorização de Incidentes: Trata-se de definir se o incidente deverá ser atendido imediatamente ou se poderá esperar um pouco, utilizando-se critérios relacionados à urgência e ao impacto. Um incidente urgente é aquele que precisa ser atendido rapidamente, enquanto um incidente impactante é aquele que poderá gerar grandes riscos ao negócio da PRX Capital. Os incidentes poderão, ainda, serem classificados de acordo com um dos seguintes níveis de priorização: "muito baixo", "baixo", "normal", "alto" e "muito alto".
- Diagnóstico Inicial de Incidentes: Busca-se aqui, de fato, entender o incidente que foi reportado, de forma a abarcar todo o processo de procura por uma solução que realmente resolva o chamado de incidente efetuado por usuário do armazenamento em nuvem da PRX Capital. Realiza-se a uma análise da base de dados de incidentes da PRX Capital destinada a ser utilizada como fonte de conhecimento para solução dos mesmos.
- Escalada de Incidentes: Caso o encarregado de resolver o incidente não tenha êxito na consecução dessa tarefa, a mesma será atribuída a um 2º (segundo) nível, de suporte, nos termos dos manuais detidos pelo provedor do armazenamento em nuvem contratado pela PRX Capital.
- Resolução de Incidentes: Ocorre quando os chamados são realmente solucionados, seja pelo 1º (primeiro) ou 2º (segundo) níveis de atendimento, quando devem ser registradas as informações relevantes sobre o incidente e sua respectiva resolução.
- Fechamento de Incidentes: Trata-se do encerramento do chamado de incidente, que deve ser registrado na base de dados futuras consultas.

Identificação dos Riscos

O TI é responsável pelo mapeamento dos riscos internos e externos, dos equipamentos e softwares utilizados pela PRX Capital.

A Diretoria de Compliance, Risco e PLD da PRX Capital é responsável pela análise dos riscos mapeados e pela implantação/investimento dos processos que precisam de proteção e monitoramento.

No âmbito de suas atividades, a Gestora 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 Gestora, 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 Gestora e as tecnologias
- desenvolvidas internamente e por terceiros, suas ameaças possíveis e sua vulnerabilidade;

- Processos e Controles: processos e controles internos que sejam parte da rotina
- das áreas de negócio da Gestora; e
- Governança da Gestão de Risco: a eficácia da gestão de risco pela Gestora quanto às ameaças e planos de ação, de contingência e de continuidade de negócios.

Ações de Prevenção e Proteção

Todo o procedimento operacional é monitorado pela área especializada em TI da PRX Capital.

Monitoramento e Testes

O TI é a responsável pelo monitoramento e emite relatórios semanais e mensais que medem a disponibilidade dos servidores e das estações de trabalho contendo a relação das atualizações realizadas e possíveis pontos de vulnerabilidades, serviços e atualizações dos antivírus.

Plano de Respostas

A capacidade e efetividade do plano de resposta é vital para proteger as informações e os recursos de informação da PRX Capital, clientes e usuários.

Todo o procedimento operacional é monitorado. Os recursos de TI são monitorados por sistemas automatizados que fornecem informações atualizadas sobre a indisponibilidade dos serviços com registro de incidentes para providências e encaminhamento de soluções e está preparada para possibilitar um plano de resposta de forma ágil e consistente.

Caso a PRX Capital sofra algum ataque cibernético que ocasione a perda de acesso aos sistemas, os responsáveis por cada área estão autorizados a acionar a equipe de help desk de TI e ativar os acessos aos sistemas de back-up em nuvem da PRX Capital, de forma que todo o trabalho operacional possa ser mantido.

Propriedade Intelectual

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 Gestora, tais como minutas de contrato, memorandos, cartas, 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 PRX 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 Gestora, devendo todos os documentos permanecer em poder e sob a custódia da PRX Capital, sendo vedado ao Colaborador, inclusive, apropriar-se de quaisquer desses documentos e arquivos após seu desligamento, salvo se autorizado expressamente pela PRX Capital e ressalvado o disposto abaixo.

O Colaborador, deverá assinar o o Termo de Confidencialidade, Compromisso e Responsabilidade da PRX Capital, sendo um documento apartado, porém é integrante a esta Política, confirmando

que:

- 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
- quaisquer alterações, adaptações, atualizações ou modificações, de qualquer forma ou espécie, em tais documentos e arquivos, serão de propriedade exclusiva da Gestora, sendo que o Colaborador não poderá apropriar-se ou fazer uso de tais documentos e arquivos alterados, adaptados, atualizados ou modificados após seu desligamento, exceto se aprovado expressamente pela PRX Capital.

13. Teste De Varredura para Detecção de Vulnerabilidades

O objetivo da análise de vulnerabilidade é reduzir o risco em relação aos incidentes de segurança, seja tanto na rede interna quanto na externa, é necessário detectar essas possíveis falhas e corrigi-las para garantir que a rede esteja em um nível de segurança adequada.

A análise de vulnerabilidade visa detectar falhas em diversos componentes como: aplicações, softwares, equipamentos, sistemas operacionais, dentre outros. Deve-se fazer continuamente o processo de verificação e análise da rede, para que ela fique sempre atualizada e livre de acessos não permitidos e indesejáveis. Essa análise pode ser feita local e/ou remota.

Os testes de invasão ou vulnerabilidade têm como objetivo descobrir e explorar falhas de segurança, permitindo assim que as organizações corrijam seus pontos de vulnerabilidade.

O teste de invasão faz-se uso de todos os artifícios que um hacker geralmente usaria. Em outras palavras, o que se tem são simulações controladas de ataques reais, objetivando a avaliação da segurança da organização e relatando as deficiências tanto da estrutura física quanto lógica.

O teste de invasão envolve análise de rede e de portas, identificação de sistemas, vulnerabilidades em sistemas sem fios, verificação de serviços (como site da PRX Capital, correio interno, servidor de nomes e documentos visíveis), determinação de vulnerabilidades e identificação dos exploits, verificação manual das vulnerabilidades, verificação das aplicações, verificação de firewall, revisão das políticas de segurança, verificação de sistemas de detecção de intrusos, revisão de sistemas de telefonia, obtenção de informação sobre a gestora, engenharia social, verificação de sistemas considerados confiáveis, análise de senhas, revisão da política de privacidade, análise de cookies e bugs no site, revisão de arquivos de log e até mesmo análise do lixo corporativo.

Antivírus

Antivírus dos servidores e estações são atualizados automaticamente e a varredura por vírus é feita diariamente nas estações e servidores.

Estabelecimento de Mecanismos de Rastreabilidade

Todo usuário é adequadamente identificado, sendo responsável pela utilização do equipamento no desempenho de suas atividades diárias.

Os softwares referentes aos controles de ativo e passivo, possuem trilha de auditoria para assegurar o rastreamento de eventos, possibilitando:

- Identificação do usuário;
- Data e horário de ocorrência do evento;
- Identificação do evento (inclusão, alteração ou exclusão).

No caso da rede interna de computadores, são utilizadas trilhas de auditoria com os seguintes registros de acessos: usuário, data e horário.

14. Proteção de Dados

De acordo com a Lei n° 13.709, de 14 de agosto de 2018 ("LGPD"), a PRX Capital irá sempre atuar na busca de investimento em cibersegurança e implementação de sistemas de compliance efetivos para prevenir, detectar e remediar violações de dados pessoais.

A segurança da informação prevista na LGPD, em relação aos Dados Pessoais, mesmo após seu término, é responsabilidade dos Agentes de Tratamento de Dados Pessoais ou qualquer outra pessoa que intervenha no Tratamento.

A PRX Capital possui Política de LGPD que abrange também os Dados Pessoais que sejam tratados pela Gestora, e trazem as medidas estabelecidas para a proteção dos dados.

A Gestora está comprometida em preservar a privacidade de dados pessoais e de dados sensíveis que forem coletados ou aos quais tiver acesso em função do uso do site ou por conta do desempenho de suas atividades, e com o cumprimento das leis e regulamentos em vigor. É importante observar que o escopo da proteção de dados pessoais no âmbito da PRX Capital está, em grande parte, limitado aos dados pessoais de seus Colaboradores e de pessoas físicas e jurídicas com as quais tiver estabelecido relações jurídicas. Também estão abrangidos por esta proteção os dados de candidatos às vagas na PRX Capital, de fornecedores e outros com os quais a Gestora manteve contato para atender alguma demanda relevante e específica.

A PRX Capital (na qualidade de Controlador) é responsável pela guarda dos Dados Pessoais coletados e armazenados em seus sistemas, sendo que os Dados Pessoais devem ser tratados com base nas hipóteses permitidas na legislação.

Nas hipóteses em que o Tratamento de dados não tiver sido previamente mapeado pela PRX Capital, o Encarregado deverá ser acionado para definir as providências a serem tomadas para garantir o correto Tratamento dos Dados Pessoais.

As normas de segurança e padrões técnicos para o gerenciamento de riscos de segurança cibernética e para mitigação de riscos estão previstos na presente Política.

15. Arquivamento de Informações

De acordo com o disposto nesta Política, 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 ou investigação em torno de possíveis investimentos e/ou clientes suspeitos de corrupção e/ou lavagem de dinheiro.

16. Considerações Finais

Todas as dúvidas sobre as diretrizes desta Política podem ser esclarecidas com a gestão de Compliance, Risco e PLD da PRX Capital.

17. Manutenção dos Arquivos

A PRX Capital manterá armazenado todos os arquivos eletronicamente, pertinentes ao processo de Compliance desta política, pelo prazo mínimo de 05 (cinco) anos, conforme legislação vigente.