

# POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

*KIRON CAPITAL GESTÃO DE RECURSOS LTDA*

Versão 1.0  
Janeiro de 2019

# POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

## 1 OBJETO

---

Esta Política tem por objetivo definir os princípios e métricas da KIRON que nortearão a avaliação de riscos de segurança da informação, o controle e prevenção de ataques, a resposta adequada a incidentes, bem como a conscientização de todos os parceiros, sócios, diretores, funcionários (permanentes ou temporários) e estagiários da KIRON (coletivamente, "Colaboradores") com relação à importância da adoção de práticas de segurança.

Por meio desta política, busca-se controlar, monitorar e proteger:

- (i) A base de informações dos clientes (atuais e potenciais) da KIRON;
- (ii) Banco de dados (incluindo informações históricas) utilizados pela empresa;
- (iii) Plano de negócios da KIRON e suas estratégias de investimentos;
- (iv) Propriedade Intelectual, como metodologias de apreçamento que sejam desenvolvidos pelos Colaboradores da KIRON;
- (v) Listas de usuários e senhas; e
- (vi) Acessos a pastas e documentos sigilosos, bem como sistemas de negociação de ativos utilizados pela KIRON.

### 1.1 Conceitos e Definições

A seguir temos todos os vocábulos técnicos utilizados na elaboração desta Política:

- Backup: cópias de dados realizadas com o intuito de proteger aqueles dados contra possíveis falhas ou perdas;
- CSI – Comitê de Segurança da Informação: grupo de colaboradores designados para tratamento de assuntos específicos de Segurança das Informações;
- CSIRT – Computer Security Incident Response Team: grupo técnico responsável por tratar e responder a Incidentes de Segurança da Informação;
- Login: processo de acessar um sistema informático restrito. Normalmente este processo necessita de um processo de autenticação e autorização;
- Logs: registros de eventos observados em determinados sistemas informatizados (por exemplo: uma tentativa de acesso em um sistema irá gerar um registro – LOG – desta ação).
- Passphrase: é um tipo de senha que, ao invés de ser baseado em uma palavra, utiliza frases inteiras para aumentar a complexidade e segurança da senha;
- Restore: ato de restaurar os dados de uma cópia de segurança (Backup);
- SMS – Short Message Service: serviço de telefones celulares digitais para envio de mensagens curtas;
- SNMP – Simple Network Management Protocol: tipo de protocolo de gerenciamento e monitoramento de dispositivos de redes;
- SPAM: termo utilizado para caracterizar mensagens indesejadas que são, normalmente, enviadas de forma automatizada para vários usuários diferentes;
- Token: dispositivo que pode ser eletrônico (físico) ou virtual (aplicativo) que gera senhas de utilização única para serem utilizados em conjunto com as senhas pessoais de cada usuário;
- Usuário da Rede: qualquer indivíduo ou instituição que tenha acesso autenticado aos recursos da rede corporativa da KIRON
- Usuário de Sistema: qualquer indivíduo ou instituição que tenha acesso autenticado aos sistemas disponibilizados pela KIRON;
- VPN – Virtual Private Network: é uma rede de comunicações privada construída sobre uma rede de comunicações pública (como por exemplo, a Internet);

# POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Esta Política deve ser lida em conjunto com o Manual de *Compliance* da KIRON (“**Manual**”). Termos definidos, quando não aqui referidos, devem ter os significados a eles atribuídos no Manual.

## 2 Princípios

---

A KIRON tem a ciência de que gestoras de investimento não podem ignorar o risco cibernético. A segurança das informações é uma demanda cada vez mais presente, tanto por parte dos reguladores, quanto de clientes e parceiros, de modo que a ação pró-ativa na gestão do risco cibernético é uma ferramenta crucial para garantir a confidencialidade, a integridade e a disponibilidade dos dados e dos sistemas da KIRON e de seus clientes.

A KIRON adota os seguintes princípios para garantir o sucesso da implementação desta Política de Segurança das Informações na empresa:

- A Diretoria Executiva da KIRON deve apoiar ativamente as ações de Segurança das Informações e também as de Comunicação Interna, de forma a demonstrar aos demais colaboradores o comprometimento necessário para atingir os objetivos e metas definidos;
- O acesso às informações e aos recursos computacionais corporativos deverá ser liberado somente após o colaborador revisar e declarar ciência de suas responsabilidades referentes ao cumprimento das diretrizes desta Política de Segurança das Informações;
- Nos casos onde houver violação, não cumprimento ou risco de uma brecha de Segurança da Informação, o CSI (Comitê de Segurança da Informação) da KIRON deverá ser imediatamente comunicado para poder dar início às ações de resposta ao incidente em questão;
- Quaisquer casos omissos nesta norma deverão ser resolvidos pelo CSI com apoio do Diretor de Compliance, ou da Diretoria Executiva.

### 2.1 Comitê de Segurança da Informação (CSI)

O Comitê de Segurança da Informação (CSI) é composto pelos Colaboradores da KIRON e pelo Diretor de *Compliance* e tem por objetivo fortalecer os processos e a cultura de segurança da informação, bem como as seguintes responsabilidades e atribuições:

- Assessorar na implementação das ações de segurança da informação da empresa;
- Solicitar e acompanhar ou realizar investigações e avaliações para identificar se a política em vigor está adequada às necessidades da empresa e se está sendo devidamente seguida;
- Em caso de um incidente de segurança, acionar a empresa terceira responsável pelo Tratamento e Resposta a Incidentes (CSIRT).

# POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

## 3 Diretrizes e Procedimentos para observância

---

A seguir estão as diretrizes mínimas que devem ser seguidas para cada tema, considerando as melhores práticas e normas específicas de Segurança:

### 3.1 Tratamento da Informação

Toda e qualquer informação disponibilizada pela KIRON aos seus colaboradores deverá ser tratada em caráter restrito, sendo vedada a disponibilização ao público, salvo se aprovado pela Diretoria Executiva ou pelo Comitê de *Compliance*.

Os colaboradores devem observar também as restrições aplicáveis ao tratamento de Informações Confidenciais ou dos Produtos KIRON, tal como definidos no Manual de Compliance da KIRON.

### 3.2 Tratamento da Incidentes

Em caso de um possível incidente, o responsável pela identificação do incidente em questão deverá comunicar o CSI imediatamente para que este possa acionar o CSIRT (empresa terceira específica para o Tratamento e Resposta a Incidentes).

É de responsabilidade do CSIRT receber, analisar e responder às notificações e atividades relacionadas aos incidentes de segurança na rede de computadores da KIRON, assim como coletar e anexar todas as evidências necessárias para a solução ou prevenção dos incidentes;

O processo de resposta a incidentes desempenhado pelo CSIRT deverá ser constantemente acompanhado e documentado pelo CSI da KIRON, de forma a aferir os serviços realizados e absorver as lições aprendidas de cada situação.

### 3.3 Controles de Acesso

São as regras de acessos à rede corporativa:

- Os acessos lógicos, locais ou remotos, à Rede Corporativa da KIRON deverão ser realizados somente para os interesses específicos dos negócios da empresa;
- O acesso à Rede Corporativa deverá ser realizado através de diferentes perfis de acesso, específicos para cada colaborador ou utilizador, sendo de responsabilidade da Diretoria Executiva definir as atribuições e atualizações dos perfis em questão;
- Cada perfil terá suas atribuições que concederão acesso aos diferentes recursos tecnológicos da rede corporativa, conforme definição da Diretoria Executiva;
- As redes e recursos destinados aos visitantes da empresa deverão ser utilizados somente pelo seu público alvo;
- As técnicas de autenticação e autorização empregadas para validar a identidade dos usuários na rede são **Nome de Usuário** e **Senha Pessoal**. Em casos de acesso remoto à Rede Corporativa, será obrigatório um segundo fator de autenticação, que deverá ser apresentado no momento da autenticação em conjunto com a senha pessoal;

## POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

- Os acessos realizados a sistemas que exijam autenticação e autorização deverão ser sempre encerrados quando finalizados ou bloqueados temporariamente durante interrupções no serviço ou em ausências dos colaboradores responsáveis;

### 3.4 Acesso à Internet e utilização de E-mail Corporativo

- A vigência do acesso à conta de correio eletrônico corporativa deve ser vinculada ao período estipulado no contrato firmado entre o usuário e a KIRON;
- O acesso à internet e a conta de correio eletrônico corporativo disponibilizado aos usuários da rede (WiFi e cabeada) da KIRON são de uso pessoal e intransferíveis, sendo o seu titular o único e total responsável pelas ações e possíveis danos causados à Instituição ou a terceiros por meio de seu uso;
- A utilização da internet e do correio eletrônico corporativo é uma concessão da KIRON, não um direito do usuário da rede e será obrigatoriamente cancelada quando do desligamento ou ao final da vigência do contrato firmado com o colaborador;
- É vedada a utilização dos serviços concedidos pela KIRON para acessar, receber, armazenar ou enviar mensagens com códigos maliciosos, materiais pornográficos, ofensas, ações criminosas ou ilegais, que façam apologia ou incitação à violência, que não respeitem os direitos autorais, os objetivos comerciais particulares ou que contribuam com a continuidade de correntes de mensagens eletrônicas e SPAM;
- O acesso à internet e ao correio eletrônico corporativo poderá ser monitorado e restringido pela KIRON a qualquer momento;
- Todos os usuários deverão se submeter aos controles implementados nas redes corporativas, de forma que a utilização de sistemas que forneçam formas de evasão destes controles seja considerada uma infração grave desta Política;
- Nos casos de suspeita de infração das Diretrizes Gerais da Política de Segurança das Informações em vigor, a KIRON poderá acessar a caixa postal corporativa do usuário da rede em questão, bem como solicitar um relatório com informações detalhadas dos sites acessados e todas as ações realizadas por ele durante a utilização dos serviços corporativos.

### 3.5 Proteção e utilização de senhas

Todas as senhas de usuários e sistemas devem seguir as seguintes diretrizes:

- No mínimo 12 caracteres alfanuméricos;
- Caracteres maiúsculos e minúsculos;
- No mínimo um número;
- No mínimo um caractere especial (!@#\$\$%^&\*()?.,);
- Quando possível, deverá ser baseada em frases (*passphrases*);
- Não ser baseada em palavras conhecidas;
- Não deve conter informações pessoais como aniversário, nomes, etc.;
- Não deve conter informações corporativas como nomes, endereços, sistemas, funções, etc.;
- Não ser baseada em padrões ou sequências de qualquer tipo;
- Contas de usuário que possuam privilégios de acesso a sistemas através da hierarquia de grupos (Serviço de Diretório) ou de programas específicos (por exemplo: SUDO) devem utilizar senhas diferentes de todas as outras contas que o usuário possuir para acesso aos sistemas;

Usuários não devem utilizar as suas senhas corporativas em contas externas que não sejam relacionadas à KIRON (por exemplo: redes sociais, e-mail pessoal, etc.). Quando possível, deve ser evitada a prática de utilizar senhas repetidas em diferentes sistemas corporativos. Todas as senhas de usuários (por exemplo: e-mail, web, Windows, etc.) devem ser alteradas, no mínimo, uma vez a cada 12 meses.

# POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

A equipe do **CSIRT** poderá realizar, de forma periódica ou aleatória, tentativas de quebra e adivinhação de senhas. Caso uma senha seja descoberta ou quebrada durante estas tentativas, o usuário será requisitado a alterar a senha para uma nova que esteja de acordo com as diretrizes deste documento.

## 4 Gestão de Riscos

---

A gestão de riscos deve utilizar como objetos de análise (i) as Atividades de Gestão e as Atividades de Empresa (tais como definidos no Código de Ética da KIRON), (ii) as instalações físicas e suas adjacências onde se encontram as atividades críticas, (iii) a infraestrutura de Tecnologia da Informação necessária e (iv) os recursos humanos que suportam estas atividades.

Como procedimentos para o gerenciamento de riscos cibernéticos, a KIRON adota dois enfoques complementares, demonstrados abaixo:

### 4.1.1 Gestão de Continuidade

A KIRON deve adotar as seguintes práticas para garantia de continuidade e segurança cibernética:

- Utilizar mecanismo de salvamento (*backup*) e restauração dos dados (*restore*) para todos os serviços e produtos desenvolvidos pela KIRON, bem como sua base de dados;
- Garantir que todos os recursos de tecnologia da informação, quando compatíveis, estejam devidamente configurados para manter registros (logs) de todos os eventos significativos para a segurança (logins, tentativas de acesso, alterações em geral, etc.);
- Revisar, atualizar e testar as medidas de cibersegurança implementadas anualmente, ou sempre que houver mudanças significativas das atividades que suportem os produtos e serviços da KIRON.
- Assegurar que o desenvolvimento de novos produtos, serviços e negócios inerentes às operações da KIRON seja feito de forma a atender essa Política de Cibersegurança, bem como assegurar que de mudanças em produtos e serviços já existentes mantenham-se em conformidade com quesitos de segurança, qualidade, eficiência e continuidade operacional;
- Comunicar imediatamente qualquer incidente que apresente risco de continuidade às áreas responsáveis (**CSI** e **CSIRT**), de forma a permitir o início imediato das providências cabíveis através do acionamento dos respectivos planos de continuidade ou recuperação;
- Documentar o impacto de qualquer possível interrupção das atividades que suportam os produtos e serviços críticos da KIRON, nos termos do Plano de Contingência da KIRON;
- Identificar soluções táticas que suportem a restauração das atividades exigidas dentro do tempo de recuperação desejado, no caso de possíveis indisponibilidades;
- Estabelecer um canal de comunicação eficiente, independente e em tempo integral, para atendimento e orientação nos casos de incidentes que possam colocar em risco a segurança do patrimônio ou das informações da KIRON;

### 4.1.2 Auditoria e Conformidade

A KIRON tem por política realizar inspeções independentes, conduzidas por um auditor no mínimo uma vez a cada biênio, com objetivo de testar a adequação dos recursos de tecnologia da informação, para (i) assegurar o cumprimento das Diretrizes e Procedimentos dessa Política de Segurança das Informações, bem como (ii) atualizar e recomendar quaisquer alterações nos controles, políticas e procedimentos adotados.

Os registros de auditoria deverão ficar armazenados na sede da KIRON por prazo não inferior a dois anos.

Versão:	1.0
Página:	6 de 7

# POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

## 5 Penalidades

---

No caso do não cumprimento ou violação das diretrizes pertencentes a esta Política, a KIRON poderá aplicar sanções e outras medidas que a Diretoria julgar necessárias, como por exemplo: desligamento imediato por justa causa, ressarcimento de prejuízos financeiros, recursos legais por danos morais, etc.

## 6 Revisões Periódicas

---

A Política de Segurança das Informações da KIRON deve estar sempre atualizada e alinhada com os interesses e necessidades da empresa. O CSI em conjunto com o Diretor de *Compliance* revisará a Política de Cibersegurança no mínimo anualmente e, sempre que uma alteração for realizada, aprovada e colocada em vigor, as alterações deverão ser amplamente divulgadas para que todos os Colaboradores tenham a oportunidade de revisar e atestar a sua ciência a respeito das novas normas implementadas ou das que foram atualizadas.