POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

SUMÁRIO

1. INTRODUÇÃO

A Política de Segurança da Informação da Ceres Asset Gestão de Investimentos Ltda. (“Ceres Asset”) aplica-se a todos os sócios, colaboradores, prestadores de serviços, clientes e parceiros de negócio, incluindo trabalhos executados externamente ou por terceiros que utilizem o ambiente de processamento da Ceres Asset, ou ainda que acesse informações a ela pertencentes. Todo e qualquer usuário de recursos computadorizados inseridos no ecossistema de negócios da nossa instituição, tem por responsabilidade zelar, proteger e reportar incidentes referentes à segurança ou integridade das informações e dos equipamentos e plataformas de tecnologia da Ceres Asset.

2. OBJETIVOS

A Política de Segurança da Informação da Ceres Asset visa proteger as informações de propriedade e/ou sob guarda da Ceres Asset, garantindo a disponibilidade, integridade, confidencialidade, legalidade, autenticidade e auditabilidade de tais informações.

Sendo assim, nenhuma informação confidencial deve, em qualquer hipótese, ser divulgada a pessoas, dentro ou fora da Ceres Asset, que não necessitem de, ou não devam ter acesso a tais informações para desempenho de suas atividades profissionais relacionadas a esta instituição.

Qualquer informação sobre a Ceres Asset, ou de qualquer natureza relativa às atividades da empresa e a seus sócios, prestadores de serviços, clientes e parceiros de negócio, obtida em decorrência do desempenho das atividades normais do colaborador, só poderá ser fornecida ao público, mídia ou a demais órgãos caso autorizado pelo Diretor de Risco e Compliance.

3. SEGURANÇA DA INFORMAÇÃO

As medidas de segurança da informação utilizadas pela Ceres Asset têm por finalidade minimizar as ameaças ao patrimônio, à imagem e aos negócios da empresa.

É terminantemente proibido que os colaboradores, clientes, prestadores de serviços ou parceiros de negócio façam cópias ou imprimam os arquivos utilizados, gerados ou disponíveis da Ceres Asset e circulem em ambientes externos à empresa com os mesmos, sem prévia autorização do Diretor de Risco e Compliance. Isso porque tais arquivos contêm informações que são consideradas informações confidenciais.

A proibição acima referida não se aplica quando as cópias ou a impressão dos arquivos forem em prol da execução e do desenvolvimento dos negócios e dos interesses da Ceres Asset. Nestes casos, quem estiver na posse e guarda da cópia ou da impressão do arquivo que contenha a informação confidencial será o responsável direto por sua boa conservação, integridade e manutenção de sua confidencialidade. Ainda, nas dependências da Ceres Asset, qualquer impressão de documentos deve ser prontamente retirada da máquina impressora, pois podem conter informações restritas e confidenciais.

O 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, sendo recomendável o seu descarte total.

Adicionalmente, os colaboradores devem se abster de utilizar pen-drives, HD externo ou quaisquer outros meios que não tenham por finalidade a utilização exclusiva para o desempenho de sua atividade na Ceres Asset.

É proibida a conexão de equipamentos na rede da Ceres Asset que não estejam previamente autorizados.

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

O acesso a sites e blogs, bem como o envio ou repasse por e-mail de material que contenha conteúdo discriminatório, preconceituoso, obsceno, pornográfico ou ofensivo também é

terminantemente proibido, como também o envio ou repasse de e-mails com opiniões, comentários ou mensagens que possam denegrir a imagem e afetar a reputação da Ceres Asset.

Programas instalados nos computadores, principalmente via internet (downloads), sejam de utilização profissional ou para fins pessoais, devem obter autorização prévia dos sócios. Não é permitida a instalação de nenhum software ilegal ou que possuam direitos autorais protegidos.

Todo conteúdo que está na rede pode ser acessado pelo Diretor de Risco e Compliance caso haja necessidade, inclusive e-mails. Arquivos pessoais salvos em cada computador poderão ser acessados caso seja necessário. A confidencialidade dessas informações deve ser respeitada e seu conteúdo será disponibilizado ou divulgado somente nos termos e para os devidos fins legais ou em atendimento a determinações judiciais ou administrativas.

4. SISTEMAS E BACKUPS

Todos os dados da Ceres Asset são protegidos por sistemas automatizados de backup realizados diariamente que garantem a recuperação rápida do ambiente dentro de Data Center.

De forma a preservar os sistemas e informações da Ceres Asset, acesso ao Data Center é realizado apenas por funcionários autorizados.

A Ceres Asset adota procedimentos internos que visam garantir a confidencialidade e integridade das informações corporativas. A rede da Ceres Asset não é acessada sem autorização do(s) responsável(is) pela infra-estrutura de TI, os e-mails são guardados por 10 anos com estrutura na nuvem.

5. MONITORAMENTO E TESTES

O Diretor de Risco e Compliance adotará as seguintes medidas para monitorar

determinados usos de dados e sistemas em um esforço para detectar acessos não autorizados ou outras violações potenciais, em base, no mínimo, anual.

Mediante ocorrência de descumprimento, suspeita ou indício de descumprimento de quaisquer das regras estabelecidas nesta Política ou aplicáveis às atividades da Ceres Asset que cheguem ao conhecimento do Diretor de Risco e Compliance, de acordo com os procedimentos estabelecidos nesta Política, o Diretor de Risco e Compliance poderá se utilizar dos registros e sistemas de monitoramento eletrônico e telefônico acima referidos para verificar a conduta dos colaboradores envolvidos.

Todo conteúdo que está na rede poderá ser acessado pelo Diretor de Risco e Compliance, caso haja necessidade. Arquivos pessoais salvos em cada computador poderão ser acessados caso o Diretor de Risco e Compliance julgue necessário.

A confidencialidade dessas informações deve ser respeitada e seu conteúdo será disponibilizado ou divulgado somente nos termos e para os devidos fins legais ou em atendimento a determinações judiciais.

O Diretor de Risco e Compliance poderá utilizar as informações obtidas em tais sistemas para decidir sobre eventuais sanções a serem aplicadas aos colaboradores envolvidos. A Ceres Asset se reserva ainda o direito de realizar inspeções periódicas com base nos seus sistemas de monitoramento eletrônico e telefônico.

O Diretor de Risco e Compliance deverá elaborar e manter arquivados relatórios descritivos dos resultados dos testes acima realizados. O Diretor de Risco e Compliance (ou pessoa por ele incumbida) adotará as seguintes medidas para monitorar determinados usos de dados e sistemas em um esforço para detectar acessos não autorizados ou outras violações potenciais, em base, no mínimo, anual: deverá verificar, por amostragem, as informações de acesso ao espaço do escritório, a desktops, pastas e sistemas, de forma a avaliar sua aderência às regras de restrição de acesso e escalonamento.

O Diretor de Risco e Compliance deverá elaborar e manter arquivados relatórios descritivos dos resultados dos testes acima realizados, caso seja encontrada qualquer inconsistência ou irregularidade. Ainda, ele poderá adotar medidas adicionais para monitorar os sistemas de computação e os procedimentos aqui previstos para avaliar o seu cumprimento e sua eficácia.

Qualquer suspeita de infecção, acesso não autorizado, outro comprometimento da rede ou dos dispositivos da Ceres Asset (incluindo qualquer violação efetiva ou potencial), ou ainda no caso de vazamento de quaisquer informações confidenciais, mesmo que de forma involuntária, deverá ser informada ao Diretor de Risco e Compliance prontamente. O Diretor de Risco e Compliance determinará quais membros da administração da Ceres Asset e, se aplicável, de agências reguladoras e de segurança pública, deverão ser notificados.

Ademais, o Diretor de Risco e Compliance determinará quais clientes ou investidores, se houver, deverão ser contatados com relação à violação.

O Diretor de Risco e Compliance responderá a qualquer informação de suspeita de infecção, acesso não autorizado ou outro comprometimento da rede ou dos dispositivos da Ceres Asset de acordo com os seguintes critérios: (i) avaliação do tipo de incidente ocorrido (por exemplo, infecção de malware, intrusão da rede, furto de identidade), as informações acessadas e a medida da respectiva perda; (ii) identificação de quais sistemas, se houver, devem ser desconectados ou de outra forma desabilitados; (iii) determinação dos papéis e responsabilidades do pessoal apropriado; (iv) avaliação da necessidade de recuperação e/ou restauração de eventuais serviços que tenham sido prejudicados; (v) avaliação da necessidade de notificação de todas as partes internas e externas apropriadas (por exemplo, clientes ou investidores afetados, segurança pública); (vi) avaliação da necessidade de publicação do fato ao mercado, nos termos da regulamentação vigente, (por exemplo: em sendo informações confidenciais de fundo de investimento sob gestão da Ceres Asset, a fim de garantir a ampla disseminação e tratamento equânime da informação confidencial); e (vii) determinação do responsável (ou seja, a Ceres Asset ou o cliente ou investidor afetado) que arcará com as perdas decorrentes do incidente.

A definição ficará a cargo da área de Risco e Compliance, após a condução de investigação e uma avaliação completa das circunstâncias do incidente.

6. VIGÊNCIA E ATUALIZAÇÃO

Esta política será revisada periodicamente, e sua alteração acontecerá caso seja

constatada necessidade de atualização do seu conteúdo. Poderá, ainda, ser alterada a qualquer tempo em razão de circunstâncias que demandem tal providência.

7. HISTÓRICO DE ALTERAÇÕES

Versão	**Data**	**Descrição da Atualização**	**Data de término**
1	6/12/21	1ª habilitação ANBIMA	7/3/22
2	8/3/22	Ato declaratório início da gestora	10/10/22
3	11/10/22	Atualizações diretoria de compliance & risco	30/9/23
4	30/9/23	Segregação do Código de Ética e Conduta	30/9/25
[•]	[•]	[•]	[•]