MOAT CAPITAL GESTÃO DE RECURSOS LTDA.

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA

Versão Atualizada

29 – JAN - 19

Av.Brig. Faria Lima, 3015 – 11º andar – Jd. Paulistano - São Paulo/SP fundos@moat.com.br +55 11 3181-8727

Índice

APRESENTAÇÃO

A Política de Segurança da Informação da Moat Capital ("Moat"), aplica-se a todos os sócios, Colaboradores, prestadores de serviços, sistemas, incluindo trabalhos executados externamente ou por terceiros que utilizem o ambiente de processamento da Moat Capital , ou que acesse informações a ela pertencentes. Todo e qualquer usuário de computadorizados ou digitais da nossa instituição tem a responsabilidade de proteger a segurança e a integridade das informações e dos equipamentos de informática.

OBJETIVOS

A Política de Segurança da Informação da Moat Capital visa proteger as informações de sua propriedade e/ou sob sua guarda, garantindo a disponibilidade, integridade, confidencialidade, legalidade, autenticidade e auditabilidade das mesmas.

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

Qualquer informação sobre a Moat Capital , ou de qualquer natureza relativa às atividades da empresa e a seus sócios, colaboradores e clientes, 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 Riscos e *Compliance*.

SEGURANÇA DE INFORMAÇÕES

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

É terminantemente proibido que os Colaboradores façam cópias ou imprimam os arquivos utilizados, gerados ou disponíveis da Moat Capital e circulem em ambientes externos à empresa com os mesmos, sem prévia autorização do Diretor de Riscos e *Compliance*. Isso porque tais arquivos contêm informações que são consideradas informações confidenciais e/ou sensíveis. Cabe ressaltar que, em relação a informações de caráter sensível ou confidencial da empresa ou de clientes, estas serão armazenados em diretórios de rede com acesso restrito, e controlado pela equipe de Riscos e *Compliance* da Moat Capital .

A proibição acima referida não se aplica quando as cópias ou a impressão dos arquivos forem em pro da execução e do desenvolvimento dos negócios e dos interesses da Moat Capital . Nestes casos, o Colaborador que 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, qualquer impressão de documentos deve ser prontamente retirada da máquina impressora, pois podem conter informações restritas e confidenciais, mesmo no ambiente interno da Moat Capital .

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, disquetes, fitas, discos ou quaisquer outros meios que não tenham por finalidade a utilização exclusiva para o desempenho de sua atividade na Moat Capital .

É proibida a conexão de equipamentos na rede da Moat Capital que não estejam previamente autorizados. Novos equipamentos e/ou sistemas deverão ter suas

configurações pela equipe de TI. Todo acesso a USB para armazenamento e bloqueado via software nos equipamentos.

Cada Colaborador é responsável por manter o controle sobre a segurança das informações armazenadas ou disponibilizadas nos equipamentos que estão sob sua responsabilidade. Será obrigatória a alteração de senha de acesso aos equipamentos (login de usuário) ao menos a cada três meses, utilizando modelo de definição de senha de difícil identificação por parte de potenciais "hackers" externos. Tal processo será auditável e rastreável eletronicamente baseado no sistema de logon do sevidor e serviços de informação.

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 Moat Capital .

Programas instalados nos computadores, principalmente via internet (downloads), sejam de utilização profissional ou para fins pessoais, devem obter autorização prévia, além de avaliação de segurança pela empresa contratada para prover suporte de TI. Não é permitida a instalação de nenhum software ilegal ou que possuam direitos autorais protegidos, ou mesmo legal, sem prévia autorização do Diretor de Riscos e *Compliance*. Não e permitido a instalação de software nos equipamentos sendo restrito a equipe de tecnologia.

Todo conteúdo que está na rede pode ser acessado pelos sócios ou pelo Diretor de Riscos 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. O acesso a rede e restrito baseado na liberação definida previamente.

Por fim, convém ressaltar que a Moat Capital conta com sistemas e ferramentas contratados para arquivamento (rede), firewall, antivírus, backup, prevensão de invesão e linha de contingência.

SERVIÇOS DE REDE

As redes de serviços são seguimentadas para garantia a segurança e desempenho entre elas. Está implantado um sistema de prevensão de invasão na rede e nos equipamentos para garantir a segurança da informação e disponiblidade de serviços.

ARMAZENAMENTO DE DADOS

O armazenamento de dados (backup) é realizado diariamente em cloud e locamente sendo disponivel para restore após liberação do responsável de segurança da informação.

INSTALAÇÕES FISICAS TECNOLOGIA / ACESSO FISICO.

Para garantia o ambiente em alta disponiblidade esta implantado um nobreak central para assegurar problemas de energia até a entrada do gerador. O sistema de ar condicionado está implantado no CPD. O acesso fisico ao CPD é controlado e autorizado somente pessoas da equipe de tecnologia da informação e Compliance.

INDISPONIBILIDADE DE ACESSO A INFORMAÇÃO

Em caso de problemas de indisponibilidade de acesso a informação e acinado o processo de plano crises sendo avalidado o impacto sobre o negocio.

TREINAMENTO DE SEGURANÇA DAS INFORMAÇÕES

A Moat Capital entende essencial que o seu treinamento anual, supervisionado pelo Diretor de Riscos e *Compliance*, abranja todos os preceitos contidos na presente política, de modo que seus Colaboradores estejam sempre cientes e consonantes os procedimentos de segregação e segurança das informações.

RELATÓRIO DE TESTES DE SEGURANÇA DAS INFORMAÇÕES

Anualmente, a Moat Capital realizará testes dos seus sistemas de segurança de informações, bem como de todos os preceitos contidos na presente política, incluindo, mas não se limitando apenas aos procedimentos de descarte de informações pelos Colaboradores, individualização dos usuários, dentre outros.

Todos os resultados desses testes, bem como os procedimentos para saneamento de eventuais problemas, serão descritos no Relatório Anual de Controles Internos da Moat Capital .

Estes testes serão realizados pela equipe de suporte de TI contratada, e buscará cobrir os seguintes ponts:

- identificação e avaliação de potenciais riscos cibernéticos, envolvendo ativos de hardware e software, além de processos que necessitem de proteção. Importante estimar impactos financeiros, operacionais e reputacionais em caso de evento;

- estabelecimento de medidas de prevenção e mitigação de riscos identificados na atividade de identificação de riscos, de forma buscar evitar eventuais ataques cibernéticos aos dados e equipamentos da empresa;

- detecção de possíveis anomalias e/ ou fragilidades no ambiente tecnológico, incluindo acessos não permitidos, usuários não cadastrados, e dispositivos não autorizados;

- criação de um plano de resposta e recuperação de incidentes, que contenha comunicação interna e externa, se necessário. Tal plano será elaborado em conjunto entre as áreas internas de Riscos e Compliance, e da empresa de TI contratada, e terá testes anuais para validar sua eficiência. O plano identificará papéis e responsabilidades, com previsão de acionamento de colaboradores e contatos externos;

- manter tal programa de segurança cibernética atualizado, identificando novos e potenciais riscos, ativos e processos.

As documentações relacionadas aos planos definidos e testes realizados, assim como os resultados auferidos e ações corretivas e mitigantes, deverão ser mantidas em diretório interno da área de Riscos e Compliance como evidência em eventuais questinamentos internos ou de órgãos reguladores ou autorreguladores.

Os temas relacionados à segurança da informação e cibernética serão tratados no Comitê Trimestral de Riscos e *Compliance*, de forma ordinária, ou mesmo em reunião específica, em casos de eventos extraordinários, para que sejam tomadas de forma tempestiva medidas de recuperação, limitação de danos, e resposta relevante.

VIGÊNCIA E ATUALIZAÇÃO

Esta Política será revisada anualmente, 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.