Política de Segurança Cibernética

Tecnologia da Informação

Versão Consolidada: 2.0

Data da Aprovação: 01/10/2020

Aprovado por: Diretoria

Conteúdo

1. Escopo

Esta Política de Segurança Cibernética ("Política") aplica-se a:

- Tullett Prebon Corretora de Valores e Câmbio Ltda. e ICAP do Brasil Corretora de Títulos e Valores Mobiliários Ltda., em conjunto adiante denominadas "TP ICAP".

- Todos os colaboradores da TP ICAP, incluindo funcionários de qualquer subsidiária da qual a TP ICAP detenha participação de controle, bem como consultores e terceiros contratados, independentemente de sua localização, função, cargo e grau, os quais são coletivamente mencionados neste documento como "Áreas de Negócios" e/ou "Colaboradores".

1.1.1. Os requisitos de controle determinados por esta Política são aplicáveis a todos os níveis de tecnologia, incluindo aplicativos, redes, sistemas operacionais, bancos de dados, *hardware* dentre outros, a menos que seja explicitamente declarado de outra forma.

1.1.2. Esta Política deve ser lida e interpretada em conjunto com os documentos listados neste documento, e tem como objetivo definir os requisitos básicos para prevenir, detectar, e responder a riscos e ameaças de cibersegurança, além de assegurar a confidencialidade, a integridade e a disponibilidade dos dados e dos sistemas de informação utilizados.

1.1.3. A capacidade da TP ICAP para prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados com o ambiente cibernético estão descritas a seguir, e evidenciadas com base nas medidas e controles existentes.

2. Definições

Ataque cibernético: é a ação praticada por *hackers* que consiste na transmissão de arquivos maliciosos que infectam, danificam e roubam informações de banco de dados. Ou seja, o ataque cibernético é um risco chave que a TP ICAP enfrenta ao gerenciar dados eletronicamente, sobre as interfaces, redes e aplicações públicas e não públicas que utiliza para intermediar negócios em nome de seus clientes.

Vulnerabilidade: pode ser entendida como uma fragilidade inerente a um ativo de informação que, uma vez explorada ou aliada a uma ameaça, possa causar incidentes de segurança ou trazer prejuízo para a integridade do sistema. As vulnerabilidades podem ser de inúmeros tipos: humanas, técnicas, físicas, de mídia, de comunicação, etc.

Risco de segurança cibernética: é definido como o risco de perda para os negócios e/ou clientes da TP ICAP resultante de ações cometidas ou facilitadas através do uso de sistemas de tecnologia em rede. Isso inclui perda resultante de tentativas de ataque eletrônico a:

- Sistemas ou dados mantidos dentro desses sistemas, que são de propriedade da TP ICAP.
- Transações e/ou dados de clientes mantidos dentro de uma tecnologia utilizada pela TP ICAP.
- Disponibilidade, integridade e confidencialidade dos serviços eletrônicos ofertados pela TP ICAP a seus clientes.
- Infraestrutura de tecnologia crítica da qual a TP ICAP depende.

TI : Departamento de Tecnologia da Informação da TP ICAP.

3. Gestão do acesso às informações

3.1. **Controle de Acessos**

As informações de um sistema e ou qualquer outro instrumento que contenha dados geridos pela TP ICAP são controladas, monitoradas e restringidas através de Controle de Acesso exercido pela Gerência de Tecnologia da Informação.

3.2. **Classificação das Informações**

Todas os dados (informações) criados, gerenciados, recebidos e processados pelos Colaboradores da TP ICAP, independente se por meio físico e ou eletrônico, devem ser identificados e rotulados adequadamente – de acordo com os critérios de classificação pré estabelecidos pela instituição.

4. Dos procedimentos e controles

Esta Política estabelece requisitos mínimos de controle para garantir que o seu objetivo seja atendido, especialmente reduzir a vulnerabilidade da instituição perante os riscos cibernéticos a que está exposta, de acordo com o apetite de risco da TP ICAP, que devem ser atendidos por todas as Áreas de Negócios e Colaboradores.

Para implementação dos requisitos de controle desta Política foram estabelecidas três "camadas" de segurança cibernética que, combinados, constituem os pilares de segurança cibernética a fim de mitigar todos os riscos associados, a saber:

- Identificação.
- Controle/Monitoramento.
- Reporte/Escalonamento.

Tais camadas foram constituídas para que seja garantida a segurança na infraestrutura tecnológica da TP ICAP através de um gerenciamento efetivo de identificação, monitoramento, tratamento e respostas a eventuais incidentes, objetivando assim minimizar os riscos de falhas e maior governança nas redes de comunicação da instituição.

Desta forma, para identificar e controlar os riscos de segurança cibernética associados às operações contínuas da tecnologia da TP ICAP, inclusive no desenvolvimento de sistemas de informação seguros e na adoção de novas tecnologias empregadas nas atividades da instituição, foram definidos requisitos de controle, cujo os principais destacam-se abaixo, não excluindo, portanto, outros dispostos nas demais políticas de Tecnologia da Informação da TP ICAP.

4.1. **Autenticação**

As informações e ambientes tecnológicos da TP ICAP somente podem ser acessados por pessoas autorizadas, geridas através do Controle de Acesso.

Para tanto, a TP ICAP possui diretrizes em seu Manual de Segurança da Informação que visam garantir que qualquer indivíduo seja identificado unívoco e inequivocamente (identificação), que a identidade das pessoas ou recurso seja expressamente comprovada (autenticação), que somente as pessoas e recursos permitidos tenham acesso aos ativos (autorização) e que as

informações sejam acessadas apenas por aqueles expressamente autorizados (confidencialidade).

Os clientes e usuários são responsáveis pelos atos executados com seu identificador (login e senhas), que são pessoais e intrasferíveis, bem como utilizadas para sua identificação/autenticação individual no acesso a informações e recursos de tecnologia da TP ICAP.

Recomendamos que os seguintes cuidados e precauções sejam tomadas com relação as senhas pessoais:

- Mantenha a confidencialidade, memorize e não registre a senha em lugar algum;
- Alterar a senha sempre que existir qualquer suspeita do comprometimento dela;
- Elaborar senhas de qualidade, de modo que sejam complexas e de difícil adivinhação;
- Impedir o uso do seu equipamento por outras pessoas, enquanto este estiver conectado/ "logado" com a sua identificação;
- Bloquear sempre o equipamento ao se ausentar da mesa;
- Sempre que possível, habilitar um segundo fator de autenticação (Por exemplo: SMS, Token e etc.)

4.2. **Comprometimento de dados**

Refere-se ao risco dos dados da TP ICAP e de seus clientes, armazenados em plataformas tecnológicas, serem comprometidos, roubados e/ou divulgados a uma parte não autorizada. Para mitigar este risco, a TI da TP ICAP deve:

- Monitorar e relatar todos os incidentes de perda de dados identificados na TP ICAP aos canais apropriados.
- Implementar e gerenciar um processo formal para monitorar e restringir o número de usuários que podem acessar sites de mídia social ou baixar conteúdo hospedado em sites de terceiros (incluindo o uso de e-mail de terceiros) para qualquer uma das redes internas da TP ICAP, o que inclui a revisão dos privilégios de acesso concedidos a cada 1 (um) ano, no mínimo.
- Restringir os privilégios dos usuários nas estações de trabalho para evitar que usuários não autorizados instalem softwares e executem arquivos não licenciados ou aprovados previamente

4.2.1. Negação de serviço ("DoS"): também definido como "stress de site", configura-se com a indisponibilidade de sistemas e serviços online, intencionalmente provocada e oriunda de ataques cibernéticos direcionados ou aleatórios. A TI da TP ICAP deve estabelecer processo para coletar, analisar e relatar as informações sobre possíveis ataques de negação de serviço, ou eventuais vulnerabilidades dos serviços das Áreas de Negócios da TP ICAP.

Quando apropriado, devido à classificação de dados ou serviços, a TP ICAP deverá implementar e operar processo de mitigação de negação de serviço que inclua a tentativa de absorver os efeitos de um ataque de negação de serviço antes que tal tráfego afete quaisquer serviços relevantes ou armazenamentos de dados da TP ICAP.

4.3. **Criptografia**

Para proteger a confidencialidade de informações sensíveis, preservar a integridade de informações críticas e confirmar a identidade do originador da transação ou comunicação, podem ser utilizados mecanismos de criptografia.

A TP ICAP utiliza-se da arte e a ciência de utilizar matemática para tornar a informação segura e criar um grande nível de confiança no meio eletrônico.

4.4. Engenharia social

A engenharia social, no contexto de segurança da informação, consiste à técnica pela qual uma pessoa procura persuadir outra, muitas vezes abusando da ingenuidade ou confiança do usuário, para obter acesso aos sistemas e dados confidenciais da TP ICAP (vazamento de dados).

O ataque de engenharia social pode se dar de diversas formas, destacando-se:

4.4.1. *Phishing* - Ataque cibernético visando enganar usuários através de envio de e-mails maliciosos, instalação de *softwares* maliciosos com o objetivo de obter dados pessoais.

4.4.2. Spam – E-mails não solicitados possuindo tipicamente conteúdo com fins publicitários ou suspeitos, visando a propagação de códigos maliciosos e disseminação de golpes.

4.4.3. Falso contato telefônico: Técnicas utilizadas para conseguir dados pessoais, como senhas, token, código de identificação do aparelho celular (IMEI) ou qualquer outro tipo de informação para a prática da fraude.

A TP ICAP busca prevenir vulnerabilidades à ataques de engenharia social projetados para permitir acesso não autorizado à dados, cujas medidas envolvem monitorar e relatar/capacitar de forma ostensiva os usuários dos serviços e/ou a tecnologia (internos e voltados para a internet) da TP ICAP que estão expostos a vulnerabilidades de segurança da Engenharia Social classificadas como altas/críticas.

4.5. Atualização de softaware, testes e varreduras

Para controlar os riscos de segurança cibernética associados às operações contínuas da tecnologia da TP ICAP, foram definidos procedimentos e controles para detectar eventuais vulnerabilidades, cujos principais destacam-se abaixo, não excluindo, portanto, outros dispostos nas demais políticas de Tecnologia da Informação da TP ICAP.

4.5.1. Proteção contra vírus e ataques – Todo equipamento deve ter um programa antivírus instalado, sendo os softwares antivírus atualizados diária, automática e obrigatoriamente. Caso o colaborador receba algum e-mail alertando sobre vírus, não deverá passá-lo a outras pessoas, pois a maioria desses alertas é falso. Permanecendo a dúvida, deverá entrar em contato com a equipe de suporte técnico para maiores explicações. Adicionalmente, a TP ICAP realiza testes de intrusão, que tem como objetivo detectar, rastrear e relatar de forma preventiva eventuais vulnerabilidades de intrusão classificadas como altas/críticas, que forem identificadas dentro do teste de intrusão global anual.

4.5.2. Atualização e Aquisição de Software – Arquivos e softwares só podem ser baixados com prévia aprovação do Departamento de Tecnologia. Quando tal ação representar obrigação onerosa e formal à TULLETT e à ICAP, é obrigatória a aprovação da respectiva Diretoria Comercial e Jurídica. Não é permitido obter softwares, imagens, etc. (download) destas fontes para uso nas Corretoras a não ser que haja uma permissão explícita por parte do seu dono. Recomenda-se a todos os colaboradores que devem ler e compreender todas as restrições dos direitos autorais do software. Caso a empresa não possa cumprir com as condições estipuladas, não deve ser feito download e não deve utilizar o material.

4.5.3. Controle de acesso: A TP ICAP possui diretrizes formais de segurança da informação para controle de acesso aos seus ativos da informação de forma física ou lógica, portanto, padronizar a administração de acessos e recursos de tecnologia e controlar os acessos físicos nas dependências da instituição.

A área de Compliance, juntamente com a Área de Tecnologia, são os responsáveis respectivamente por normatizar, administrar o processo de acessos a sistemas e recursos informatizados das Corretoras, bem como o monitoramento dos acessos concedidos. Todos os computadores, redes, sistemas e softwares estão sujeitos à monitoração e, portanto, a Tullett e a ICAP reservam-se o direito de manter, a seus critérios, histórico de acessos e transações realizadas.

O monitoramento dos acessos físicos é feito através dos sistemas, que registram as movimentações nos diversos ambientes da empresa, inclusive, nos ambientes segregados (Mesa de Operações, CPD, etc). Sempre que julgar necessário, o Compliance faz testes periódicos para certificar o funcionamento das ferramentas de acessos, bem como atestar que os acessos aos ambientes das Corretoras são respeitados e limitados às pessoas devidamente autorizadas.

4.6. Malware

Refere-se a ataques cibernéticos que comprometem a segurança da rede interna (de produção e corporativa) da TP ICAP, por meio da implantação de software mal-intencionado.

A TP ICAP desenvolve medidas para monitorar e relatar os serviços e/ou a tecnologia (internos e voltados para a internet) que estão expostos a vulnerabilidades de segurança classificadas como altas/críticas.

4.7. Rastreabilidade

Para preservação da integridade das informações, especialmente a segurança das informações sensíveis, a TP ICAP pode estabelecer trilhas de auditoria automatizadas para componentes de sistema, que tem como objetivo rastrear a autenticação de usuários (tentativas válidas e inválidas), acesso à informações e as ações executadas pelos usuários, incluindo criação ou remoção de objetos do sistema.

4.8. Segmentação de redes

Todos os acessos aos recursos das redes sob responsabilidade da TP ICAP, que são devidamente segmentadas por áreas com controle de acesso, devem ser solicitados através de processo específico e comunicado a Gerência de Tecnologia.

Os controles de segmentação de rede visam permitir que desenvolvedores e administradores de sistemas tomem decisões mais eficazes e implementem funcionalidades de segurança consistente e simples de usar em vários aplicativos e sistemas de negócios em toda a organização.

A redes são segmentadas em Produção, Desenvolvimento, Homologação e Desmilitarizada (DMZ) e constituem estratégia de mitigação de vulnerabilidades, visando garantir a segurança e a segmentação nos perfis de acesso de cada ambiente.

Computadores conectados à rede corporativa não devem ser acessíveis diretamente pela Internet, exceto através de conexão especifica para tanto, devidamente homologada e autorização pela Tecnologia da Informação da TP ICAP.

Para solicitação de criação, alteração e exclusão de regras nos firewalls e ativos de rede, o requisitante deve encaminhar pedido à área de Segurança da Informação, que fará a análise e aprovação, enviando para que seja executada pela área de TI.

4.9. Logs e Backup

A importância de logs e backups na administração de sistemas e dados nunca pode ser minimizada. Visa garantir que, em caso de emergência, informações essenciais ou sistemas

podem ser restaurados de acordo com o cronograma crítico, bem como tem o condão de ajudar a identificar ameaças que possam levar a um incidente de segurança, manter a integridade das informações importantes à segurança e apoiar a realização de análises e investigações forenses.

Os controles adotados para mitigação de vulnerabilidades, inclui os voltados para a rastreabilidade da informação, que busca garantir a segurança das informações sensíveis.

Cada usuário tem um diretório no servidor de arquivos. Todos os documentos que digam respeito ao negócio deverão ser salvos neste diretório.

O backup de dados pessoais nas estações de trabalho é de total responsabilidade do usuário.

O backup dos servidores é executado pela equipe de Tecnologia da Informação seguindo os procedimentos definidos pela área e respeitando os prazos de retenção dos reguladores.

4.10. **Prestadores de Serviços / Terceiros**

As diretrizes da presente política aplicam-se a todos os colaboradores da TP ICAP, incluindo terceiros (prestadores de serviços, consultores, temporários ou outras denominações).

A existência das diretrizes estabelecidas com base nesta Política e a necessidade do cumprimento de suas premissas devem ser referenciadas nos contratos e acordos com os fornecedores, clientes e terceiros, bem como nas obrigações dos demais colaboradores das Corretoras, de forma que cada um saiba suas obrigações, direitos e deveres com a segurança das informações.

5. Do gerenciamento de vulnerabilidades

A Gestão de vulnerabilidades refere-se ao risco dos dados da TP ICAP e de seus clientes, armazenados em plataformas tecnológicas, serem comprometidos, roubados e/ou divulgados a uma parte não autorizada. Além dos procedimentos e controles adotados previstos nesta política, para mitigar este risco, a TI da TP ICAP deve implementar e monitorar processos para a identificação proativa de vulnerabilidades técnicas, priorização da correção de vulnerabilidades identificadas usando uma abordagem baseada em risco e resolução oportuna de vulnerabilidades por meio de aplicação de patches de segurança ou implementação de outros controles de compensação apropriados.

Os funcionários declaram-se cientes de que a TP ICAP reserva-se o direito de monitorar quaisquer atividades por eles desenvolvidas, através de todos os meios disponibilizados, tais como, e-mail corporativo, telefone, mensageria, com o intuito de identificar atividades suspeitas ou em desconformidade com esta Política, demais Políticas ou Manuais Internos e legislações existentes.

Todos a quem se dirige esta política são responsáveis por monitorar e relatar os ativos e serviços de tecnologia (internos e externos) expostos a vulnerabilidades de segurança classificadas como críticas.

5.1. **Níveis de classificação de vulnerabilidade**

A TP ICAP classificará eventuais vulnerabilidades identificadas como de baixa, média ou alta vulnerabilidade a depender da situação especifica e impacto nos negócios da instituição.

5.2. Das vulnerabilidades identificadas

Uma vez identificada alguma vulnerabilidade, seja nos ativos e serviços de tecnologia (internos e externos), o TI da ICAP deve registrar onde ocorre, identificar os riscos diretos e indiretos, definir plano de ação, nível de classificação e respectivo prazo para correção e indicar um responsável pela gestão da vulnerabilidade.

O responsável pela gestão, assim como o TI da TP ICAP devem efetuar o monitoramento da adequação quanto ao nível de controle e cumprimento desta Política, assim como do Manual de Segurança da Informação.

6. Do gerenciamento de incidentes

Violações significativas da segurança interna ou externa devem ser respondidas de forma eficaz e oportuna pela TI da TP ICAP, com a implementação e o monitoramento de processos, que incluem as seguintes etapas:

- A documentação do incidente, indicando causa (quando possível);
- A atribuição de classificação de impacto apropriada;
- O escalonamento e a resolução.

Qualquer suspeita de que está havendo um incidente de segurança deverá ser informada a Gerência de Tecnologia. Nenhum colaborador deverá investigar por conta própria, ou tomar ações para se defender do ataque, a não ser que seja instruído desta forma pela Gerência de Tecnologia. A Gerência de Tecnologia está capacitada para conter as exposições, analisar os impactos das Corretoras e conduzir investigações, coletando evidências para possíveis ações jurídicas. Os incidentes são acompanhados mensalmente no comitê de Risco e *Compliance.*

6.1. Classificação de incidentes

Os incidentes que são identificados pelos alertas são classificados com relação ao impacto de acordo com os critérios adotados pela TP ICAP. Para o seu grau de relevância serão considerados aspectos como comprometimento de dados de clientes e impacto ao sistema financeiro.

6.2. Reporte / Escalonamento

Todos os incidentes passam por um processo de tratamento e comunicação, onde são registradas todas as informações pertinentes aos incidentes como causa, impacto, classificação etc., de acordo com o procedimento operacional.

Os seguintes requisitos de controle foram definidos para gerenciar o escalonamento de riscos cibernéticos até o nível apropriado:

6.2.1. Violações cibernéticas bem-sucedidas: as violações bem-sucedidas do sistema interno de defesa da TP ICAP devem ser adequadamente registradas e monitoradas pela TP ICAP, com emissão de relatório para coletar, analisar e relatar todas as violações sofridas pela TP ICAP (independentemente da avaliação ou da alocação da perda).

6.2.2. Quantificação de perda cibernética: eventuais perdas tangíveis ou intangíveis causadas por violações bem-sucedidas da segurança cibernética devem ser avaliadas e distribuídas para os níveis apropriados da TP ICAP, com a devida análise do relatório emitido.

6.2.3. Investigação cibernética: as investigações em curso devem ter nível apropriado de visibilidade dentro da gestão da TP ICAP, o que inclui a emissão de relatórios em que as investigações em andamento sejam reportadas aos níveis apropriados da TP ICAP.

O Diretor responsável pela presente política deverá ser comunicado na ocorrência de qualquer incidente de segurança, e será responsável por acompanhar a execução do plano de ação e de resposta a incidentes.

A TP ICAP deve elaborar anualmente, com data base o último dia do ano objeto do documento, Relatório Anual de Incidentes, para formalização da implementação do plano de ação e resposta a incidentes, caso tenham ocorrido, que deverá conter, no mínimo as seguintes informações:

- resumo dos resultados obtidos na implementação das rotinas, dos procedimentos, dos controles e das tecnologias a serem utilizados na prevenção e na resposta a incidentes;
- os incidentes relevantes relacionados com o ambiente cibernético ocorridos no período;
- os resultados dos testes de continuidade de negócios, considerando cenários de indisponibilidade ocasionada por incidentes.

O referido relatório anual sobre a implementação do plano de ação e resposta a incidentes deverá ser submetido para o comitê competente (se existente) e apresentado a Diretoria da TP ICAP até 31 de março do ano seguinte ao ano da data-base.

7. Da cultura de Segurança Cibernética

A presente política aplica-se a todas as Áreas de Negócios e Colaboradores da TP ICAP e deve ser disponibilizada em canal aberto e de fácil acesso.

Os colaboradores da TP ICAP devem receber treinamento periódico acerca dos conceitos de Segurança da Informação, através de um programa efetivo de treinamento da TP ICAP plc.

A TP ICAP tem o compromisso em manter os seus elevados padrões de atendimento e disponibilidade do serviço, sempre em conformidade com a legislação vigente, mantendo assim, à disposição de clientes e usuários, principais aspectos de segurança tecnológica em seu site, bem como, permanece à disposição através dos seus canais de comunicação, para prestação de informações acerca das precauções relacionadas a segurança cibernética na utilização pelos clientes e usuários dos seus produtos e serviços.

8.Gerenciamento da Política

8.1. **Responsabilidades**

O Diretor de TI e de Controles Internos da TP ICAP é responsável pela presente Política.

A alta administração da TP ICAP tem ciência da importância da presente política, na qual se compromete com a melhoria contínua dos procedimentos ora relacionados.

8.1.1. Departamento de Tecnologia da Informação

Tem a responsabilidade de ser a primeira linha de defesa para com os objetivos desta política e deve:

- Garantir conformidade e práticas de trabalho dentro de seus controles de forma tempestiva e assertiva;
- Realizar monitoramento de conformidade em relação aos requisitos da Política;
- Fornecer os dados do Indicador de Risco de Política ("IR") mensalmente e ou quando requisitado ao Diretor de TI e de Controles Internos, que zelará pela aderência de todas as Áreas de Negócios e Colaboradores aos requisitos determinados nesta da Política.

Não obstante as disposições acima, a Tecnologia da Informação da ICAP deve definir, operar e revisar regularmente todos os controles definidos nesta Política para garantir que eles estejam em conformidade com os requisitos aqui estabelecidos e a evidência de tais revisões deve ser mantida.

A TI deve identificar exceções à Política que exigem uma aceitação de risco. Estes casos devem ser avaliados, documentados e requerem aprovação da Diretoria da TP ICAP. As Aceitações de Risco devem ser revisadas e ratificadas pelo menos anualmente.

8.1.2. Departamentos Jurídico e de Compliance

São responsáveis por auxiliar o Departamento de Tecnologia da TP ICAP em qualquer questão regulatória e ou de controle, bem como realizar comunicação de requisitos legais e regulamentares relativos a riscos e controles de segurança cibernética.

8.2. **Revisão**

A Política deve ser revisada e atualizada conforme necessário e reconfirmada sua validade, exatidão e integridade anualmente. Qualquer alteração introduzida que seja considerada substancial deve ser analisada pelo Comitê de Risco da TP ICAP e aprovada pelo Diretor de TI e de Controles Internos.

8.3. **Violação da Política**

A violação desta Política pode resultar na vulnerabilidade da TP ICAP a ataques cibernéticos, o que pode levar a danos significativos, incluindo, mas não se limitando, a perdas financeiras, multas regulatórias, danos à reputação e perda de negócios. Por isso, a violação desta Política pode ensejar em ações disciplinares e/ou legais aplicadas pela TP ICAP contra o(s) violador(es).

8.4. **Dúvidas**

Dúvidas relacionadas ao conteúdo desta Política deverão ser direcionadas à TI.

9. Documentos Relacionados

Além das disposições previstas nesta política, a TP ICAP poderá adotar diretrizes previstas em outros documentos, mencionados ou não nesta política, deste que relacionados a Segurança da Informação e Gestão de Riscos da instituição.