1. OBJETIVO

Esta política tem por objetivo estabelecer os fundamentos e diretrizes, a serem obrigatoriamente observados pela companhia e todos os seus colaboradores, de segurança cibernética que assegurem a confidencialidade, a integridade e a disponibilidade de dados e sistemas de informação, observando a natureza das operações, a complexidade dos produtos, dos serviços, das atividades e dos processos havidos na e pela corretora, bem como o porte, perfil de risco, modelo de negócio e a sensibilidade dos dados e das informações sob responsabilidade da instituição; tudo em conformidade com a Resolução n° 4.658 do Banco Central do Brasil, de 26 de abril de 2018, e visando detectar, prevenir e mitigar a vulnerabilidade a incidentes relacionados com o ambiente cibernético.

2. CONCEITO

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.

No arcabouço de Segurança Cibernética estes e alguns outros conceitos são essenciais para a compreensão do processo, e por isso são a seguir definidos:

i. **Confidencialidade:** Garantir que as informações sejam acessadas apenas por pessoas autorizadas;
ii. **Integridade:** Garantir que as informações, tanto em sistemas quanto em bancos de dados, estejam em um formato verdadeiro e correto para seus propósitos originais;
iii. **Disponibilidade:** Garantir que as informações e os recursos estejam disponíveis para aqueles que precisam deles quando necessário;
iv. **Ataques Cibernéticos:** Os ataques cibernéticos mais comuns, podem ser realizados através de *software* maliciosos que são desenvolvidos para corromper computadores e redes de dados, que podem ser realizados através de métodos de manipulação para obtenção de informações confidenciais, como senhas e dados pessoais, ou que possa visar a negação ou atraso de acessos aos serviços ou sistemas da instituição;
v. **Incidente de Segurança da Informação:** Um incidente de segurança da informação pode ser definido como qualquer evento adverso, confirmado ou sob suspeita, relacionado a

segurança, que pode comprometer a Confiabilidade, Integridade e/ou Indisponibilidade das informações;

vi. **Malware**: *softwares* desenvolvidos para corromper os computadores e redes, como:

a) **Vírus**: *software* que causa danos à máquina, rede, *softwares* e banco de dados;

b) **Cavalo de Troia**: aparece dentro de outro *software* criando uma porta para a invasão do computador;

c) ***Spyware***: *software* malicioso para coletar e monitorar o uso de informações;

d) ***Ransomware***: *software* malicioso que bloqueia o acesso aos sistemas e base de dados, solicitando um resgate para que o acesso seja reestabelecido.

vii. **Engenharia social**: métodos de manipulação para obter informações confidenciais, como senhas, dados pessoais e número de cartão de crédito:

a) ***Pharming***: direciona o usuário para um site fraudulento, sem o seu conhecimento;

b) ***Phishing***: links vinculados por e-mails, simulando ser uma pessoa ou empresa confiável que envia comunicação eletrônica oficial para obter informações confidenciais;

c) ***Vishing***: simula ser uma pessoa ou empresa confiável e, por meio de ligações telefônicas, tenta obter informações confidenciais;

d) ***Smishing***: simula ser uma pessoa ou empresa confiável e, por meio de mensagens de texto, tenta obter informações confidenciais;

e) Acesso pessoal: pessoas localizadas em lugares públicos como bares, cafés e restaurantes, a fim de captar qualquer tipo de informação que possa ser utilizada posteriormente para um ataque.

viii. **Ataques de DDoS (*distributed denial of services*) e *botnets***: ataques visando negar ou atrasar o acesso aos serviços ou sistemas da instituição;

ix. **Invasões (*advanced persistent threats*)**: ataques realizados por invasores sofisticados, utilizando conhecimentos e ferramentas para detectar e explorar fragilidades específicas em um ambiente tecnológico.

x. **Ataques de *Brute Force***: ataques de força bruta visando o acesso ao ambiente e aplicações, por meio, do preenchimento de usuário e senha, sendo realizadas de forma manual ou automática, por meio de *softwares*;

xi. **Informação confidencial**: definida conforme item 3.14 abaixo;

xii. **Informação restrita**: a informação que poderá ser acessada por um grupo específico de pessoas, justificada a sua necessidade;

xiii. **Informação pública**: informação que já é divulgada ao público em geral e que, portanto, se divulgada por necessidade de negócio, não provocará impactos. Para a classificação devem ser consideradas as necessidades relacionadas ao negócio, o compartilhamento ou restrição de acesso e os impactos no caso de utilização indevida das informações.

3. PROCEDIMENTOS E CONTROLES

3.1. Autenticação

a) Toda aplicação que manipular informações não públicas deve exigir a autenticação do usuário antes do acesso à informação;

b) A aplicação deverá oferecer a possibilidade de configuração de uma política de senhas em que seja possível parametrizar a quantidade mínima de caracteres no sistema;

c) Atender a requisitos de complexidade (letras maiúsculas e minúsculas, números e caracteres especiais);

d) Solicitar ao usuário a troca de senha no primeiro login;

e) Bloquear o usuário após tentativas de login incorretas, devendo ser a quantidade de tentativas parametrizável no sistema;

f) Não permitir o uso simultâneo do mesmo usuário em diferentes instâncias da aplicação;

g) A aplicação não deve resgatar a senha atual dos usuários; em caso de perda da senha o sistema deve conduzir a troca de senha;

h) As senhas dos usuários da aplicação devem ser armazenadas utilizando um algoritmo de *hash* com chave criptográfica maior que 256 bits;

i) Os servidores que utilizam sistema operacional Unix e seus derivados (Ex.: Linux, Solaris, AIX, HP-UX, Tru64) deverão ter o usuário privilegiado (*root*) controlado pela ferramenta padrão da empresa para envelopamento de senha e rastreabilidade.

3.2. Criptografia e Certificados Digitais

a) As informações sensíveis e manipuladas nas aplicações devem ser protegidas por controles criptográficos durante o seu transporte e armazenamento;

b) Não deve ser utilizado algoritmos de criptografia proprietários e/ou desenvolvidos internamente;

c) As chaves de criptografia não devem ser armazenadas (*hard-coded*) no código da aplicação;

d) O acesso à chave de criptografia deve ser protegido por controles de acesso apropriados;

e) Em aplicações Web, as chaves de criptografia devem ser armazenadas em um repositório separado dos arquivos e páginas HTML da aplicação;

f) As aplicações que utilizem certificados digitais para autenticação devem verificar os mesmos contra as listas de certificados revogados (LCR) publicados pelas Autoridades Certificadoras (AC) confiáveis. Este controle evita que certificados revogados por qualquer motivo sejam utilizados para acesso à aplicação.

3.3. Prevenção e detecção de intrusão

a) Os mecanismos de detecção devem monitorar, analisar e bloquear ações realizadas com intuito de comprometer a estrutura básica da segurança de informação de um sistema informatizado, afetando sua integridade, confidencialidade e disponibilidade;

b) Os mecanismos de detecção devem monitorar e analisar os padrões de tráfego, bem como pacotes individuais, incluindo a correspondência de endereço, cadeia de caracteres e *substring* HTTP e análise de conexão TCP;

c) Possibilitar a identificação de problemas com políticas de segurança e documentação de ameaças existentes;

d) Detecção de eventos baseados em assinatura (conhecidos) e ataques que compões eventos múltiplos;

e) Detecção e bloqueio de anomalias quando identificados ataques novos e já conhecidos.

3.4. Prevenção de vazamento de informações

a) A privacidade e proteção de dados devem ser asseguradas conforme exigido na legislação, regulamentações, políticas de grupo e, se aplicável, nas cláusulas contratuais;

b) Devem existir controles para verificação de autenticidade e integridade dos dados do sistema de forma a prevenir que qualquer ação do usuário, falha do sistema, inserção ou remoção indevida de dados possa causar inconsistência da base de dados;

c) Os dados sensíveis do arquivo de configuração das aplicações web, como *strings* de conexão, devem ser encriptados;

d) Mensagens de erro que são mostradas ao usuário devem revelar somente as informações necessárias, sem vazamento de detalhes internos do sistema na mensagem de erro;

e) Dados exportados para outros sistemas confiados deverão ser mantidos sob as mesmas condições de privacidade que o sistema de origem;

f) Os dados manipulados pelo sistema deverão ser mantidos sob o mesmo nível de integridade e confidencialidade exigido pelo nível de segurança;

g) Dados sensíveis não devem ser armazenados na aplicação final, esses dados deverão ser encriptados e armazenados no servidor;

h) Não deve ser mantido caches locais nos equipamentos dos usuários finais.

i) As informações confidenciais do cliente não deverão permanecer nos equipamentos dos usuários finais, após o encerramento do aplicativo ou browser.

3.5. Realização periódica de testes e varreduras para detecção de vulnerabilidades

A avaliação de segurança deverá ser feita de forma periódica nos sistemas que já se encontram em uso e de forma pontual nos sistemas em desenvolvimento ou de forma extraordinária quando assim for necessário. A avaliação de segurança se dará através das seguintes análises:

a) **Análise de arquitetura:**
É voltada para a análise da arquitetura de um sistema ou de um ambiente de rede a fim de verificar o nível de segurança estrutural. A análise refere-se as especificações dos requisitos de projeto da plataforma e às soluções de implementação adotadas. O resultado de uma Análise de Arquitetura identifica os potenciais elementos de vulnerabilidade da arquitetura em exame.

b) **Análise de vulnerabilidades**:
É a verificação dos serviços fornecidos por uma infraestrutura, por um sistema ou, de forma geral, por uma plataforma, a fim de pôr em evidência os pontos fracos de caráter técnico do sistema e a eficácia dos sistemas de segurança adotados. O resultado de uma atividade de análise de vulnerabilidades reporta um conjunto de vulnerabilidades com as relativas referências técnicas e nível de criticidade.

c) **Teste de invasão:**
Destina-se à pesquisa e à simulação da exploração de uma vulnerabilidade para obter o controle de um sistema ou de uma plataforma.

A atividade se baseia nas informações obtidas pela análise das vulnerabilidades e se completa com verificações manuais e com outras técnicas. O resultado de um teste de invasão fornece uma classificação e rating das vulnerabilidades observadas, as evidências da exploração delas e um plano detalhado de correção/adequação.

3.6. Proteção contra *softwares* maliciosos

a) Os *guidelines* (correções de segurança) deverão ser aplicados em todos os ativos devem ser executadas pelos responsáveis do sistema operacional;

b) Sistemas Operacionais e seus módulos não devem ser instalados com uma versão defasada;

c) Somente serviços e protocolos necessários e seguros devem ser ativados, conforme exigido para a função do sistema;

d) Todas as funcionalidades desnecessárias devem ser removidas, como scripts, drivers, recursos, subsistemas, sistemas de arquivo e servidores da Web desnecessários;

e) Somente funcionalidades relevantes para o funcionamento do sistema devem ser instaladas;

f) O sistema e todos os *softwares* que o suportam devem ser legalmente licenciados;

g) Considerar a aplicabilidade dos processos e adequações padrões da área de TI para configuração interna para todos os componentes do sistema. Certificar-se de que esses padrões abrangem todas as vulnerabilidades de segurança;

h) Os aplicativos, arquivos e serviços que não são pertinentes à funcionalidade do servidor devem ser removidos do sistema operacional;

i) Os patches de segurança do sistema operacional devem ser mantidos atualizados;

j) Acesso remoto ao sistema operacional deve ser restrito apenas à equipe de suporte responsável;

k) As contas de serviço utilizadas no sistema operacional para a execução de processos em lote (batch), scripts e serviços não devem possuir acesso privilegiado (administrativo) ao sistema operacional;

l) Os sistemas deverão ser monitorados pelas ferramentas padrão de monitoramento da Necton Investimentos;

m) Correções de segurança (patches) devem ser instaladas frequentemente ou por solicitação das áreas de TI em produtos de terceiros tais como sistemas operacionais, bancos de dados, servidores *web* e etc.;

n) Todos os Patches de correção de vulnerabilidades de segurança devem ser validados em um ambiente de testes/homologação antes de serem instalados nos servidores do ambiente de produção.

3.7. Estabelecimento de mecanismos de Rastreabilidade

a) O sistema deverá gerar logs possibilitando a rastreabilidade da ação do usuário do começo até o final de cada operação;

b) Os registros de auditoria devem ser protegidos contra acesso não autorizado e contra qualquer tipo de alteração;

c) Todas as alterações nas funções administrativas deverão ser registradas em log de auditoria;

d) Os sistemas deverão registrar em log todas as operações de eventos historicamente, mantendo por 5 anos os registros, contendo data, hora, minuto e segundo, *user id* e IP para:
   i. *Read*: Toda leitura que for feita;
   ii. *Copy*: Toda cópia que for feita total ou parcial do dado;
   iii. *Update*: Toda alteração que for feita;
   iv. *Print*: Toda vez que for efetuado uma impressão;

e) bloqueio ou exclusão de usuários não deverá acarretar em perda dos logs das operações realizadas pelos mesmos;

f) As informações sensíveis não deverão ser registradas no log em texto claro;

g) As ações dos usuários finais no sistema devem ser registradas em log de forma completa no início do processamento e ao final de cada operação;

h) Informações sensíveis ao negócio da Necton Investimentos não deverão ser gravadas em log em texto puro;

3.8. Controles de acesso e de segmentação da rede de computadores

a) A rede deve ser estruturada e segmentada através de *firewall*, com segregação entre os setores e servidores;

b) O *firewall* deve ser capaz de limitar o tráfego de informações entre departamento e dispositivos com a capacidade de realizar a filtragem de pacotes, realizar inspeções profundas e detecção de malware;

c) As instâncias de desenvolvimento, homologação e treinamento dos sistemas devem ser segregadas do ambiente de produção;

d) Não é permitido o acesso da equipe de desenvolvimento ao ambiente de produção;

e) Deverá ser implementada apenas uma função principal por servidor para evitar funções que exigem diferentes níveis de segurança coexistindo no mesmo servidor (Por exemplo, servidores da Web e servidores do banco de dados devem ser implementados em servidores distintos);

f) O acesso ao banco de dados deve ser realizado somente pela aplicação. A camada de apresentação e os usuários finais não devem ter acesso direto ao banco de dados.

g) A comunicação entre aplicação e ao banco de dados deve ser criptografada.

3.9. Cópias de segurança de dados das informações

a) A informação deve receber proteção adequada em todo o seu ciclo de vida, que compreende: Geração, Manuseio, Armazenamento e Descarte;

b) O colaborador responsável pela informação deve ter conhecimento do tempo regulatório de salvaguarda e gerenciar o seu armazenamento e descarte e, em caso de dúvida, deverá questionar formalmente o departamento Jurídico da companhia;

c) O descarte de informação confidencial deve ser efetuado utilizando máquina fragmentadora de papéis ou incineradora.

3.10. Controle de segurança das informações sensíveis

a) Informações sensíveis armazenadas em bancos de dados de sistemas de produção não devem ser copiadas para ambientes de desenvolvimento e de testes sem a aprovação da área de Segurança da Informação;

b) Informações envolvidas em transações on-line devem ser protegidas contra falhas na transmissão, rotas indevidas, alteração, duplicação, reenvio e exposição não autorizadas;

c) Deve ser garantido que os fornecedores externos não obtenham informações confidenciais ou a cópia da base de dados com informações verídicas, salvo exceções previamente autorizadas pela área de Segurança da Informação e após a assinatura de Acordo de Confidencialidade;

d) Informações confidenciais devem ser restritas aos usuários autorizados, garantindo que o acesso a informações sensíveis seja limitado a um grupo apropriado de pessoas e áreas internas, visando assegurar a proteção, o tratamento adequado e a aplicação do conceito *need to know* (mínimo acesso necessário ao desempenho das funções).

3.11. Testes de continuidade de negócios

O plano de contingência e de continuidade dos principais sistemas e serviços da companhia deverá ser implantado e testado anualmente, contemplando cenários de incidentes, a fim de reduzir riscos de perda de confidencialidade, integridade e disponibilidade dos ativos de informação. Todo o plano de contingência de continuidade dos negócios está descrito na política de plano de continuidade.

3.12. Empresas prestadoras de serviços a terceiros

a) Todo terceiro com acessos aos recursos tecnológicos deve respeitar as políticas vigentes;

b) Os contratos serão avaliados pelas áreas competentes, admitindo-se o apoio de áreas específicas visando à conformidade com a legislação em vigor, normas reguladoras e políticas vigentes;

c) É indispensável nos contratos de prestação de serviço o termo de confidencialidade e definições de SLA (*Service-Level Agreement*), estabelecido de acordo com o nível de criticidade do recurso ao negócio;

d) É dever da Necton Investimentos sempre acompanhar as atividades prestadas por terceiros;

e) Em caso de projetos longos ou com necessidade de alocação interna, o departamento de RH deve ser notificado para que todos os documentos referentes ao termo de confidencialidade sejam assinados;

f) Após o terceiro estar ciente e aceitar cumprir as regras, o departamento de RH informará os acessos devidos às áreas competentes conforme alinhamento com a área requisitante;

g) O terceiro contratado fica ciente de que ao violar qualquer política ou processo formal estará sujeito as devidas aplicações previstas em contrato e legislação vigente;

h) No encerramento de suas atividades os termos de confidencialidade permanecem vigentes e a área responsável pelo acompanhamento deve notificar o departamento de RH para solicitar a revogação dos acessos;

i) Todos os recursos fornecidos devem ser devolvidos no mesmo estado em que foram disponibilizados, sujeito à compensação a Necton Investimentos por eventuais avarias detectadas.

3.13. Segurança da nuvem

a) A adoção de serviços hospedados em nuvem privada, pública, híbrida ou em ambiente de parceiros e/ou fornecedores, deve respeitar sempre a premissa da confidencialidade, integridade e disponibilidades das informações;

b) Os serviços podem ser complementares ao *on premises*, respeitando o acesso para a rede da Necton Investimentos e as aplicações que devem ter interação;

c) Além das definições tecnológicas, os serviços devem respeitar a legislação e localidades, que estejam dentro dos acordos estabelecidos pelas autarquias responsáveis pela regulação e fiscalização de nosso mercado e atuação;

d) Para os demais detalhes e necessidades, devem ser seguidas as regras estabelecidas para a contratação de *softwares*, serviços e equipamentos.

3.14. Controles para informações classificadas como “Confidencial”

a) Informações confidenciais devem ser identificadas como tal: e-mails, apresentações, documentos;

b) Os e-mails e arquivos com informações confidenciais devem ser protegidos;

c) O acesso às informações confidenciais deve ser controlado;

d) Qualquer documento pessoal que seja disponibilizado a terceiros deve ser enviado com a identificação do terceiro, editada em marca d'água;

e) Sempre que necessário, contratos de confidencialidade da informação devem ser assinados com terceiros.

4. INCIDENTES E CONTROLE DOS EFEITOS DOS INCIDENTES RELEVANTES

4.1. Registro e Análise da causa e impacto

Ao receber a notificação, deve-se analisar a falha para identificação da criticidade, impacto, áreas afetadas e plano para correção. O plano de recuperação deve ser executado em tempo hábil para que o impacto do incidente seja minimizado.

4.2. Definição dos parâmetros de relevância

A equipe pode basear-se em notificações externas ou em um conjunto de ferramentas de monitoração. Os esforços da equipe concentram-se em identificar os sintomas do ataque e suas características, observando a severidade do incidente, ou seja, o quanto a estrutura de negócios da instituição é afetada.

4.3. Estrutura organizacional e operacional

Um incidente de segurança da informação é um evento que pode afetar a confidencialidade, integridade ou disponibilidade das informações, em qualquer formato ou em qualquer sistema de TI que a informação esteja armazenada. Qualquer funcionário, cliente ou supervisor pode notificar um incidente. Todo incidente é registrado, analisado, encaminhado para solução e, revisado. Este fluxo garante a melhoria contínua nos processos e no ambiente tecnológico da Necton Investimentos.

4.4. Prevenção e resposta a incidentes

É realizado a avaliação do processo de tratamento de incidentes e verificada a eficácia das ações adotadas. As lições aprendidas durante todo o processo serão catalogadas e propagadas na base histórica de conhecimento.

4.5. Áreas Responsáveis

A responsabilidade pela notificação de um incidente é de todos os funcionários, clientes e fornecedores. A responsabilidade pelo tratamento e análise dos incidentes é da área de segurança da Informação com o apoio das áreas envolvidas na solução (infraestrutura, banco de dados, desenvolvimento, área de negócio etc.).

4.6. Compartilhamento de informações

Os casos serão analisados e a as medidas cabíveis adotadas, bem como reporte e compartilhamento de informações a todas as áreas aplicáveis.

5. CULTURA DE SEGURANÇA CIBERNÉTICA

5.1. Programas de Capacitação

O departamento de RH é responsável por elaborar treinamentos que envolvam aspectos de segurança cibernética aos colaboradores, contendo:

a) **Abrangência**: Colaboradores, prepostos e prestadores de serviços;
b) **Aplicação**: Palestras, workshop, teste de *phishing*, quiz.
c) **Treinamento para o nível de conscientização**: *Phishing*, *Spam* e e-mails fraudulentos;
d) Aplicação de provas ou questionários para medir a conscientização ao final dos treinamentos;
e) Plano de ação para colaboradores que não atingiram o nível de conscientização mínima esperada.

5.2. Prestação de informações a clientes e usuários

A área de Tecnologia da Informação é responsável por elaborar e enviar comunicados contendo ações de conscientização, com o objetivo de disseminar a cultura de Segurança Cibernética aos clientes da Necton Investimentos.

5.3. Comprometimento da alta administração

Atingir um padrão eficiente e consistente de boas práticas para a Segurança da Informação em toda a empresa exige direcionamento claro e comprometimento por parte da alta direção. Desta forma a Necton Investimentos se compromete a atingir altos padrões de governança corporativa, tratar Segurança da Informação como elemento vital ao negócio, criar um ambiente positivo de segurança, e demonstrar a terceiros que a empresa trata a Segurança da Informação de forma profissional e compatível com sua estrutura e operações.