POLÍTICA DE SEGURANÇA

CIBERNÉTICA

Versão: 2022.1
Data Aprovação: 15/12/2022
Aprovação: DIRETORIA

1. OBJETIVO

Esta política tem por objetivo estabelecer os fundamentos associados ao processo de segurança cibernética definidos com base em princípios e diretrizes que buscam assegurar a confidencialidade, a integridade e a disponibilidade de dados e dos sistemas de informação, em conformidade com a Resolução CMN 4.893/21.

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.

Alguns outros conceitos são essenciais para a compreensão do processo, assim 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, 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: O 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 da informação.

3. ESTRUTURA ORGANIZACIONAL

A COLUNA adota modelo de estrutura descentralizada a fim de assegurar isenção ou potenciais conflitos de interesses.

4. RESPONSABILIDADE

Em linha com o escopo desta Política, segue abaixo os papéis e responsabilidades detalhados e segmentados.

4.1. Diretoria

- Revisar e atualizar esta Política anualmente ou quando necessário, em conjunto com as demais áreas integrantes;
- Deliberar sobre as decisões e ações relacionadas à segurança cibernética;
- Monitorar ativamente e tratar dos assuntos referentes ao tema em nível estratégico, tático e operacional;
- Conduzir o processo de investigação interna e apuração de causas e responsabilidades nos incidentes ou violações de segurança

- Monitorar ativamente a observância dos dispositivos contidos nesta Política;
- Definir de procedimentos e de controles voltados à prevenção e ao tratamento dos incidentes a serem adotados por empresas prestadoras de serviços a terceiros que manuseiem dados ou informações sensíveis ou que sejam relevantes para a condução das atividades operacionais da instituição;
- Fazer constar sua responsabilidade pelas informações divulgadas no relatório anual de acesso público, evidenciando a estrutura de gerenciamento desses riscos.

4.2. Tecnologia da Informação

- Definir procedimentos e controles adotados para reduzir a vulnerabilidade da instituição a incidentes e atender aos demais objetivos de segurança cibernética e publicá-los em documento interno específico para seu registro;
- Atualizar regras e procedimentos técnicos referentes a prevenção e proteção de ativos de tecnologia;
- Registrar e analisar a causa e o impacto, bem como controlar os efeitos de incidentes relevantes para as atividades da instituição e publicá-los em documento interno específico para seu registro;
- Definir os parâmetros a serem utilizados na avaliação da relevância dos incidentes e publicá-los em documento interno específico para seu registro;
- Manter soluções de prevenção e proteção de dados sempre atualizadas;
- Proteger os dados através de backups periódicos;
- Realizar diligência na contratação de serviços de terceiros, inclusive serviços em nuvem;
- Avaliar questões de segurança durante as fases de pré-projeto e desenvolvimento de novos sistemas, softwares ou aplicações.

4.3. Compliance

- Aplicar Treinamento referente ao conteúdo desta política, sempre que necessário;
- Propor sugestões para a correção tempestiva de deficiências e fraquezas eventualmente identificadas nesse processo, ou ajustes decorrentes de exigências e alterações requeridas pelo Banco Central.

4.4. Demais Áreas

- Disseminar aos colaboradores sob sua gestão, a política, controles, procedimentos e padrões que eles deverão seguir e respeitar;
- Responsabilizar-se pela propriedade das informações de sua área ou quando a classificação da informação assim exigir.
- Respeitar e cumprir todo o conteúdo disposto nesta política e nas demais políticas do Grupo;
- Ter ciência de que todas as informações geradas, acessadas, processadas, utilizadas ou armazenadas em qualquer meio ou sistema de informação, devem ser exclusivas as atividades na COLUNA
- Reportar para as áreas responsáveis qualquer violação ou incidente de segurança da informação;
- Participar dos treinamentos e disseminar a cultura e importância de todos agirem com responsabilidade no tratamento das informações.

5. DIRETRIZES

Assegurar que as informações sejam adequadamente protegidas, através dos processos e controles.

5.1. Controle de Segurança Cibernética

Os controles de segurança cibernética, devem estar alinhados e acordados entre a estrutura da instituição.

- Bancos de dados e dispositivos de rede com segurança dedicada que seja rigorosamente controlado para preservar a integridade, a confidencialidade e a disponibilidade do conteúdo;
- Manutenção e atualização dos sistemas operacionais e softwares utilizados na instituição;
- Prevenção de ameaças com firewalls, antivírus, perfis de acesso específico para os administradores dos sistemas/redes, filtros de spam, controle para uso de periféricos, soluções de prevenção e correções de vulnerabilidades e filtros de uso de internet;
- Inclusão das preocupações de segurança durante as fases de desenvolvimento de novos sistemas, softwares ou aplicações;
- Controles de auditoria, tais como sistemas de gerenciamento de senhas, logs e trilhas de acessos.

5.2. Gestão de Segurança sobre Infraestrutura, Software de Base, Configuração e Utilitários

a) Concessão de Acesso a Usuários, Registro, Manutenção e Verificação Periódica

Em função da amplitude dos acessos dos colaboradores que implementam e mantém a infraestrutura de tecnologia, sua contratação deve ser formalizada considerando a validação de perfil e idoneidade comprovados, e formalizado o seu direito de acesso e comprometimento com o sigilo de informações declarado em documento próprio, que autorize o monitoramento integral de suas atividades e comunicação, além de aceitar a responsabilidade sobre as ações que perpetrar no exercício das suas funções.

As funções de segurança exercidas pelos responsáveis pela Infraestrutura (Software e Hardware) são sujeitas a geração de Logs de atividades que serão armazenados de forma protegida e terão revisão independente pelo Gestor TI.

b) Registro, Proteção e Revisão de Registro de Eventos (Logs)

Os sistemas, utilitários como gerenciadores de banco de dados e outras ferramentas de gestão de rede, especialmente as que acessam dados em produção, geram registro de operações sensíveis feitas pelo Suporte / Gestão de Infra, e é fundamental que este Log seja mantido protegido de alteração e deleção.

Deverá ser feita revisão periódica deles, quer diretamente, quer usando rotina de extração de operações pontuais com software de extração e análise de dados.

c) Regras para Manuseio, Troca e Armazenamento de Dados

As rotinas que acessem ou alterem banco de dados e outros arquivos de informações, deverão ser mantidos os requisitos mínimos de controle como: Backup, limitação de uso, retenção de fontes e forte monitoramento de rotinas usadas no ambiente de produção, mediante a aprovação do Gestor de TI.

6. PLANO AÇÃO E RESPOSTA A INCIDENTES

Em caso de ocorrência de um incidente cibernético ou indisponibilidade de recursos computacionais, serão tomadas todas as medidas possíveis para analisar e corrigir a falha, fazer o registro, a análise da causa e do impacto e dar continuidade aos negócios sem que haja prejuízo para corretora e seus clientes.

6.1. Tratamento de Incidentes

Incidentes são interrupções de sistema não planejadas que ocorrem de várias naturezas e que afetam os negócios da Corretora, como por exemplo:

- Queda de energia elétrica
- Falha elemento de conexão;
- Servidor fora ar;
- Ausência conexão internet;
- Vazamento de dados e informações;
- Indisponibilidade de recursos computacionais;
- Sabotagem e/ou ataques.

6.2. Incidente Caracterizado

Caracterizado o incidente, devem ser tomadas as medidas imediatas, tais como:

- ✓ Iniciar a redundância de TI, redirecionar as linhas de telefone para os celulares, instruir o provedor de telefonia a desviar linhas de dados/e-mail, entre outros.
- ✓ O Diretor responsável pela Política de Segurança Cibernética avaliará o impacto do incidente nos diversos riscos envolvidos.
- ✓ Conforme a relevância (sabotagem, terrorismo) poderá ser registrado um boletim de ocorrência ou queixa crime para as devidas providências.

6.3. Recuperação

Essa fase começa após o incidente ter sido contornado, já tendo sido a contingência de TI acionada e terceiros envolvidos notificados.

6.4. Retomada

Período de transição do retorno ao modo normal de operação e podendo incluir a análise de projetos, estabelecendo a reconstrução de eventuais sistemas e eventuais mudanças e medidas de prevenção.

6.5. Comunicação ao Banco Central

A COLUNA deverá informar ao Banco Central do Brasil as ocorrências de incidentes relevantes e as interrupções dos serviços relevantes que configurem uma situação de crise.

Essa comunicação deve ser acompanhada das informações sobre o incidente ocorrido bem como das informações sobre as providências tomadas para o reinício das atividades.

7. TESTES DE CONTIGÊNCIA

A efetividade da Política, deve ser verificada por meio de testes e revisões periódicas dos controles existentes.

O plano de teste deve ser executado pela área de Tecnologia da Informação assegurando que:

- Os acessos dos colaboradores estão em conformidade com os acessos as áreas de atuação;
- Que os níveis de confidencialidade e acessos as informações confidenciais estão adequadas;
- Recursos computacionais de controle de acesso físico e lógico, estejam protegidos;
- Definição de parâmetros para avaliação dos controles de vulnerabilidade;
- Que haja rastreabilidade de registros que permitam a realização de auditorias periódicas.

8. PENALIDADES

O descumprimento de alguma regra desta política será considerado como falta grave, conforme disposto nos Código de Ética e Conduta da COLUNA ou de acordo com análise de decisão do Comitê, sujeitando o Colaborador a sanções administrativas de acordo com o grau de severidade do incidente.