Política Segurança Cibernética e da Informação

1. Objetivo

Garantir que toda informação tenha a proteção necessária no seu manuseio, tratamento e divulgação, determinando limites de comportamento e medidas a serem tomadas no caso de sua violação, em consonância com o presente documento. A Gestão de Segurança da Informação envolve os seguintes aspectos:

- Definir diretrizes e responsabilidades que devem subsidiar a elaboração de normas, procedimentos e padrões de proteção da informação, abrangendo sua geração, utilização, armazenamento e distribuição;
- Garantir a disponibilidade, integridade e confidencialidade da informação, independente do meio de armazenamento;
- Garantir que a informação seja utilizada por quem necessita para a execução de suas atividades diárias;
- Evitar que usuários possam fazer o uso da informação de forma mal-intencionada, para obtenção de benefícios próprios;
- Evitar que ataques sejam realizados por vários agentes (organizações criminosas ou hackers individuais, organismos de Estado terroristas, colaboradores, competidores etc.),
- Estabelecer subsídios para as implementações de cláusulas específicas nos contratos que visam garantir que a informação tenha a devida proteção;
- Atender aos objetivos dos negócios e aos controles internos da INTRADER DTVM.
- Atender as recomendações dos órgãos reguladores e fiscalizadores.
    - 1. Identificação/avaliação de riscos (risk assessment) – identificar os riscos internos e externos, os ativos de hardware e software e processos que precisam de proteção.
    - 2. Ações de prevenção e proteção – estabelecer um conjunto de medidas cujo objetivo é mitigar e minimizar a concretização dos riscos identificados no item anterior, ou seja, buscar impedir previamente a ocorrência de um ataque cibernético, incluindo a programação e implementação de controles.
    - 3. Monitoramento e testes – detectar as ameaças em tempo hábil, reforçando os controles, caso necessário, e identificar possíveis anomalias no ambiente tecnológico, incluindo a presença de usuários, componentes ou dispositivos não autorizados.
    - 4. Criação do plano de resposta – ter um plano de resposta, tratamento e recuperação de incidentes, incluindo um plano de comunicação interna e externa, caso necessário.
    - 5. Reciclagem e revisão – manter o programa de segurança cibernética continuamente atualizado, identificando novos riscos, ativos e processos e reavaliando os riscos residuais.

2. Diretrizes da Segurança da Informação

A INTRADER DTVM manterá sistemas confiáveis mediante utilização de padrões tecnológicos de segurança de rede, para evitar fraudes internas e invasões e garantir o sigilo de toda informação e comunicação interna e externa.

Todo usuário é adequadamente identificado, sendo responsável pela utilização do equipamento no desempenho de suas atividades diárias.

Todo novo colaborador será cadastrado nos sistemas específicos às suas funções, conforme e-mail com o formulário de cadastro de acessos da Intrader enviado pelo gestor direto do novo colaborador que deverá informar quais acessos deverão ser cadastrados/liberados, assim como o perfil adequado (consulta, alteração, aprovação ou máster).

O colaborador que for transferido de área dentro da organização, deverá ter seus acessos cancelados pela área de TI e o gestor atual do colaborador deverá enviar por e-mail à TI o formulário de cadastro de acessos da Intrader indicando os novos acessos do colaborador, para que sejam feitas as tratativas.

O colaborador que for desligado deverá ter seus acessos imediatamente cancelados, o RH deverá comunicar por e-mail a área de TI para que os procedimentos de cancelamento de acessos sejam realizados com brevidade.

Toda informação relevante deverá ser protegida, de acordo com seu grau de sigilo, integridade e disponibilidade, de forma a atender aos objetivos de segurança da informação.

São realizadas periodicamente manutenções e atualizações técnicas e de segurança, de forma a manter em plenas condições de funcionamento, os equipamentos de informática e de telecomunicações.

As ações que afetam a segurança da informação são registradas e armazenadas em arquivos magnéticos, com cópias de segurança.

Os colaboradores receberão o Termo de Compromisso comprometendo-se com a conformidade e Segurança da Informação, o qual consta anexo ao final desta política, para conhecimento e assinatura.

Somente a diretoria da INTRADER DTVM pode autorizar a divulgação pública de informações dos diversos setores, independentemente do canal de comunicação: mídia impressa, eletrônica ou qualquer outro meio.

Serão realizados testes periódicos de segurança para os sistemas de informações, em específico para os mantidos em meio eletrônico.

3. Diretrizes Operacionais

São utilizados equipamentos de rede que possibilitam a segmentação e/ou integração com outras redes, facilitando essas interligações, preservando segregado os interesses de tráfego de cada rede e evitando o congestionamento e outros efeitos que possam prejudicar seu desempenho.

4. Diretrizes Operacionais

4.1 Desenvolvimento, Aquisição e Instalação de *Softwares*

Todo desenvolvimento, aquisição, manutenção de sistema aplicativo deve zelar pela observância dos princípios de controle sobre informações processadas e armazenadas, incluindo a adequada segregação de perfis de acesso.

Esses cuidados visam impossibilitar que um único colaborador domine todas as fases de controle de uma transação, ou seja, entrada, autorização, liquidação e registro da transação.

Os *softwares* de sistemas operacionais de rede e de estações de trabalho, sistemas, utilitários de rede e similares são testados antes da sua implantação, inclusive na troca de versões.

Os testes de homologação são aplicados pelo responsável da Segurança da Informação em ambiente próprio de homologação, de forma a não gerar risco de instabilidade ou interrupção nos servidores de produção.

4.2 Segurança Física

Os colaboradores da INTRADER DTVM utilizam a senha biométrica para acesso aos ambientes do CPD visando evitar acessos indevidos por pessoas não autorizadas nas dependências da INTRADER.

Os colaboradores e prestadores de serviços de manutenção são autorizados a acessar o ambiente de CPD somente mediante acompanhamento de funcionário de TI.

4.3 Segurança na Comunicação de Dados de Voz

As instalações e equipamentos de comunicação de dados e voz são gerenciados de modo a que seja mantida a segurança e inviolabilidade das informações que trafegam por elas.

A INTRADER DTVM em conformidade com legislação vigente mantém sistema de gravações das comunicações feitas pelos seus colaboradores que utilizam os equipamentos e instalações, visando preservar a INTRADER no caso de eventuais ações dolosas ou contrárias a seus interesses comerciais e/ou operacionais.

As gravações e rotinas de monitoramento serão feitas com base em concordância expressa dos colaboradores mediante adesão e assinatura de Termo de Responsabilidade e Compromisso com as Normas de Segurança da Informação da INTRADER DTVM.

4.4 Segurança de *Hardware*

As estações de trabalho utilizadas pelos colaboradores dispõem de software instalado que protege o equipamento e a rede de dados e impossibilita, por exemplo, que os usuários instalem programas não autorizados pela área de Tecnologia da Informação.

4.5 Segurança de *Software*

O *software* de prevenção contra vírus está instalado na rede interna e nas estações de trabalho, e é atualizado conforme última versão válida.

O uso do correio eletrônico e internet pelos colaboradores são monitorados, não sendo permitido acesso a sites não autorizados, adicionalmente há restrições no recebimento e envio de arquivos anexados.

Os servidores com acesso à internet e e-mail dispõem de *firewalls* e ferramentas de segurança de rede.

4.6 Trilhas de Auditoria

Os *softwares* referentes aos controles de ativo e passivo, possuem trilhas de auditoria para assegurar o rastreamento de eventos. Essas trilhas incluem:

- Identificação do usuário;
- Data e horário de ocorrência do evento;
- Identificação do evento (inclusão, alteração ou exclusão).

No caso da rede interna de computadores, são utilizadas trilhas de auditoria com os seguintes registros de acessos: usuário, data e horário.

4.7 Normas de Backup

Foram estabelecidas as seguintes regras quanto à realização de *backups*:

- Geração diária e incremental de cópias de segurança;
- Inclusão de todas as informações armazenadas nos servidores;
- A base de dados é salva e gravada no servidor em nuvem.

O ambiente do CPD possui termômetro para marcação de temperatura e umidade relativa.

Os equipamentos estão instalados em locais adequados, protegidos dos raios solares, de altas temperaturas e de grande incidência de pó.

Os servidores e os equipamentos de telefonia instalados na sala de informática são protegidos da falta de energia elétrica por *nobreaks* que garantem:

- A uniformidade da tensão da rede, em casos de picos de energia;
- A entrada em operação das baterias, na falta de energia elétrica, com autonomia de cerca de 4 horas.

Os servidores estão instalados em sala exclusiva, climatizada, dotada de detector de fumaça e com permissão de acesso apenas às pessoas autorizadas.

4.8 Aquisição de *Hardwares*/*Softwares*

Deve-se pesquisar no mercado, dentre os fornecedores/prestadores de serviços, aqueles que apresentam condições de atender às necessidades dos usuários, elaborando cotação de preço junto a no mínimo três fornecedores, respeitando o seguinte fluxo:

Avaliar, com a participação dos diretores e usuários, os softwares selecionados, quanto aos seguintes quesitos:

- Arquitetura;
- Adequação de seus requisitos e especificações às necessidades da área/processo;
- Necessidade de customização;
- Viabilidade técnica e aderência à plataforma tecnológica;
- Facilidade de operação e de manutenção;
- Documentação e procedência;
- Licença de uso;
- Relação custo-benefício.

Propor a aquisição, preferencialmente, dos chamados *softwares* de prateleira (sistemas operacionais, editores de texto, planilhas e outros) junto com os equipamentos ou sob a forma de licença de uso, dando cobertura a cada cópia requerida conforme sua necessidade.

Apresentar à diretoria o resultado da avaliação e da cotação de preços, obtendo a aprovação para a aquisição do *hardware*/*software*.

Efetuar os testes para homologação do sistema a ser adquirido, em ambiente de teste, selecionando a melhor solução a ser indicada para aquisição.

Validar, em conjunto com os usuários, a entrada/saída de dados para garantir que eles estejam corretos e apropriados.

Obter a aprovação da contratação do sistema pelos respectivos usuários e Diretoria, após concluir por sua adequação técnica, orçamentária e negocial.

Receber o *software* entregue pelo fornecedor, juntamente com o respectivo contrato de fornecimento e, se for o caso, o contrato de manutenção e disponibilização de novas versões e atualizações.

Analisar o contrato e encaminhar para exame jurídico (se necessário), obtendo a aprovação e as assinaturas da diretoria.

Encaminhar as notas ou faturas ao departamento administrativo e financeiro para o pagamento da aquisição e da manutenção mensal.

Encaminhar a documentação relativa ao processo de aquisição ao departamento administrativo e financeiro para contabilização e para posterior arquivamento.

4.9 Contratação de Serviços

Observar os procedimentos quanto ao recebimento da solicitação do usuário.

Selecionar dentre os prestadores de serviços homologados, no mínimo 3 (três) empresas, obtendo as respectivas propostas.

Analisar as propostas em conjunto com os usuários/diretoria e adotar os procedimentos previstos para contratação do serviço, pagamento e arquivamento da documentação.

4.10 Instalação de *Hardware* e Serviços

Após a aquisição e implantação do novo *hardware* e *software*, atualizar o bem no Inventário de TI, e atualizar os controles de licenças de software.

O equipamento deve ser configurado para instalação na rede e outros links externos, mediante a instalação dos *softwares* necessários.

Habilitar os usuários para uso dos *softwares* de rede, mediante senha de acesso.

4.11 Comunicação de Dados de Voz

A manutenção da infraestrutura de comunicações da INTRADER DTVM envolve:

- Links de contingência;
- Ambiente de rede de dados;
- Linhas telefônicas;
- Sistemas de gravação de voz.

A Segurança da Informação dispõe de meios para garantir a não interrupção das comunicações, efetuar o monitoramento do desempenho dos *links* de dados, adotar providências internas junto às concessionárias para melhoria do desempenho e corrigir eventuais problemas.

5. Diretrizes Operacionais

Os procedimentos para assegurar a continuidade do negócio, estão tratados e descritos no documento “Plano de Continuidade de Negócios” desenvolvido com base na análise dos processos críticos, na análise da infraestrutura envolvida com esses processos e com base na análise da probabilidade da ocorrência de possíveis cenários que tenham impacto determinante na continuidade dos processos.

As pessoas envolvidas nos planos de contingência são adequadamente treinadas para execução das ações de sua responsabilidade, os testes são executados conforme cronograma estabelecido, os planos são atualizados sempre que necessário e os recursos alternativos (sistemas e sites de contingência) quando requeridos são disponibilizados para uso, dentro dos prazos mínimos requeridos.

O Plano de Continuidade de Negócios deverá ser objeto de testes, no mínimo anualmente, devidamente formalizado em relatório específico, cujos resultados são apresentados à diretoria para validação e comprometimento com a solução de eventuais problemas que possam resultar em riscos para a INTRADER DTVM.

No caso de interrupção das atividades da INTRADER, o plano de recuperação e continuidade será acionado conforme definido no Plano de Continuidade de Negócios - PCN da INTRADER DTVM.

6. Segurança Cibernética

A segurança cibernética é um conjunto de práticas que protege informação armazenada nos computadores e aparelhos de computação e transmitida através das redes de comunicação, incluindo a internet e telefones celulares.

Com o avanço da tecnologia e consequentemente aumento da utilização de meios de informática, os riscos de ataques cibernéticos estão mais prováveis. Quanto mais utilizamos a tecnologia mais suscetíveis a esses ataques estaremos expostos.

A INTRADER DTVM terceiriza sua área de TI, assim sendo, o processo de avaliação dos possíveis riscos, vulnerabilidades e possíveis cenários de ameaças são tratados pela empresa contratada. Ressalta-se que nada impede que exigências ou testes adicionais sejam demandados pela INTRADER.

6.1 Sistema de *Backup*

São realizados backup completo de rede diariamente, conforme agendamento. A ferramenta utilizada chama-se Cobian backup 11.

6.2 *Backup* de E-mail

O *backup* de e-mail é realizado pela empresa Nipotech que é a nossa provedora de e-mails e faz a guarda dos mesmos.

6.3 Anti Virus e Firewall

Possuímos o Firewall WatchGuardian em hardware instalado entre nossa rede interna e os links de acesso a internet.

Vale salientar que a rede interna da Intrader está totalmente protegida de acesso extenos, quando necessário um acesso é liberado no firewall o acesso através de uma VPN que é criptograda.

O FireWall tem uma interface grafica chamada Dimension que monitora sua atividades em tempo real gerando relatórios e gráficos de todo tráfego da rede, utilização dos usuários e tentativas de invasão externa.

Possuímos software de antivírus Kaspersky instalado, o mesmo foi configurado para realizar a varredura semanal ao iniciar o computador, porém o monitoramento é constante a partir do momento que o computador é ligado.

No item Diretrizes da Segurança da Informação desta Política são listadas as regras específicas para cadastramento de novos colaboradores, transferência de colaboradores entre áreas da Intrader e cancelamento de acessos para desligamento. Informamos ainda que no Código de Ética e Política de Compliance estão descritos diretrizes para a guarda e segurança de informações confidenciais e regras sobre a utilização de informações privilegiadas.

Todos os colaboradores da Intrader ao ingressar na empresa assinam o Termo de Compromisso - Confidencialidade e Segurança da Informação, Termo de Monitoramento Interno e o Código de Conduta e Ética.

6.4 Monitoramento e Testes

A empresa terceirizada de TI da INTRADER DTVM realiza diversos testes e monitoramento em seus sistemas, tais como: troca de senhas periódicas, manutenção e atualização técnica de segurança, software de proteção contra vírus, *firewall,* backups periódicos, trilha de auditoria e segurança de *hardware.* Novos colaboradores, desligados e transferências internas de área também possuem regras de segurança sistêmica e informação, tais regras estão descritas no item 2 Diretrizes de Segurança de Informação desta Política.

6.5 Plano de Resposta

No caso de invasão cibernética nos sistemas da Intrader a TI terceirizada contratada realizará imediata avaliação dos danos e definição dos processos e mecanismos que serão utilizados para sanar o problema e evitar maiores exposições, no que tange a riscos de imagem e perdas financeiras. Se necessário for, será ativado o modo contingência conforme os procedimentos previamente descritos no PCN – Plano de Continuidade de Negócios. Após a adoção de todas as medidas necessárias, o incidente será levado ao Comitê Diretivo para avaliação e, se necessária, a tomada de medidas adicionais para mitigação do risco.

6.6 Reciclagem e Revisão

A Política de Segurança Cibernética será revisada no prazo máximo de 12 meses a partir da data de publicação, onde riscos, implementações de proteção e plano de resposta serão redesenhados caso haja necessidade.

6.7 Responsável por Segurança Cibernética

A Intrader DTVM conta com serviço terceirizado de Tecnologia da Informação para atendimento das demandas imediatas. A empresa terceirizada reporta diretamente ao Diretor de Segurança Cibernética indicado em atendimento a Resolução do Banco Central n° 4658/18.

TERMO DE COMPROMISSO

CONFIDENCIALIDADE E SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA

Identificação do Funcionário

Nome:
CPF:
Departamento:

Comprometo-me a:

1**.** Executar minhas tarefas de forma a cumprir com as orientações da Política de Segurança e com as Normas e Padrões vigentes.

2. Utilizar adequadamente os equipamentos da Instituição, evitando acessos indevidos aos ambientes computacionais aos quais estarei habilitado, que possam comprometer a segurança das informações.

4. Acessar as informações somente por necessidade de serviço e por determinação expressa do superior hierárquico.

5. Manter cautela quando a exibição de informações sigilosas e confidenciais, em tela, impressoras ou outros meios eletrônicos.

7. Não me ausentar do local de trabalho sem encerrar a sessão de uso do computador ou sistema, evitando assim o acesso por pessoas não autorizadas.

8. Observar rigorosamente os procedimentos de segurança estabelecidos quanto à confidencialidade de minha senha, através dos quais posso efetuar operações a mim designadas nos recursos computacionais que acesso, procedendo a:

a. Substituir a senha inicial gerada automaticamente pelo sistema, por outra, pessoal e intransferível;

b. Não divulgar a minha senha a outras pessoas;

c. Responder em todas as instâncias, pelas consequências das ações ou omissões de minha parte que possam por em risco ou comprometer a exclusividade de conhecimento da minha senha ou das transações a que tenho acesso;

g. Reportar imediatamente ao superior imediato ou ao responsável de Governança de TI em caso de violação, acidental ou não, da minha senha, e providenciar a sua substituição.

h. Solicitar o cancelamento de meu usuário e senhas quando não for mais de minha utilização.

i. Solicitar o cancelamento de usuários/senhas solicitados para colaboradores sob minha responsabilidade, quando do seu desligamento ou término do serviço que originou a respectiva solicitação.

Tenho ciência de que a Intrader possui sistema de gravação telefônica, circuito interno de gravação de imagens, monitoramento de e-mails e qualquer outra atividade desempenhada no ambiente de trabalho da Intrader, podendo acessar tais informações a qualquer momento.

Declaro estar ciente das determinações acima, compreendendo que quaisquer descumprimentos dessas regras podem implicar na aplicação das sansões disciplinares cabíveis.

São Paulo, _____ de _____ de _____.

_____
Assinatura do Colaborador

Este Termo de Compromisso é anexo a Política de Segurança da Informação da Intrader DTVM.