ÍNDICE

1. Objetivos

A Política de Segurança da Informação e Segurança Cibernética da Guide Investimentos tem como objetivo garantir a aplicação de princípios e diretrizes para utilização das melhores práticas de governança para proteção das Informações da empresa, de seus colaboradores, de seus clientes e do público em geral.

Deve estabelecer as práticas para assegurar a confidencialidade, integridade e disponibilidade das informações, além do cumprimento de requisitos regulatórios e operacionais e proteger a empresa de riscos de imagem e legais.

2. Público alvo e abrangência

Esta Política se aplica à Guide Investimentos S.A. Corretora de Valores e a todas empresas coligadas, inclusive subsidiárias e filiais.

Deve ser de conhecimento e prática de todos administradores, empregados, estagiários, menores aprendizes e prestadores de serviços que manipulem informações da Guide Investimentos S.A. Corretora de Valores e demais empresas do Grupo.

3. Definições

A Guide Investimentos S.A. Corretora de Valores será referenciada como **Empresa**, suas subsidiárias e filiais serão referenciadas como **Unidades** e todos seus empregados, diretores, administradores, estagiários e menores aprendizes serão referenciados como **Colaboradores**.

Serão referenciados como **Usuários** todos os Colaboradores, prestadores de serviço, fornecedores e parceiros de negócio que utilizem os sistemas e serviços da Empresa e que tenham acesso às suas informações.

Esta Política de Segurança da Informação e Segurança Cibernética será referenciada como Política.

As definições desta política se aplicam à Empresa e às suas Unidades e Filiais, a não ser que estas tenham políticas ou regras próprias, referendadas por seus respectivos Comitês responsáveis.

4. Referências

4.1 Regulamentação Associada

- Resolução BACEN 4.658/18 e, complementares
- Guia de Cibersegurança ANBIMA

- Códigos ANBIMA de Regulação e Melhores Práticas
- Programa de Qualificação Operacional (PQO) – B3
- Roteiro de Testes da Auditoria Operacional - BSM
- Resolução BACEN 2.554/98
- Resolução BACEN 3.056/02
- Resolução BACEN 4.557/17
- ICVM 505/11 e, complementares
- ICVM 612/19
- ICVM 558/15
- Lei Complementar 105
- Lei 13.709/18 (Lei Geral de Proteção de Dados - LGPD)

4.2 Externas

- Norma ISO/IEC 27001
- Norma ISSO/IEC 27005

4.3 Internas

- Procedimento de gerenciamento de incidentes de segurança
- Política de continuidade de negócios
- Política de classificação de informações
- Lista de Proprietários
- Catálogo de serviços
- Lista de ferramentas e serviços homologados
- Matriz de segregação de acessos
- Procedimento para liberação de regras de *firewall*
- Política de Gerenciamento de Incidentes
- Política de cópias de segurança de informações
- Procedimento para avaliação e contratação de serviços na nuvem
- Procedimento de gestão de riscos de Segurança da Informação
- Matriz de riscos de Segurança da Informação
- Projetos de Segurança da Informação
- Política de utilização de dispositivo pessoal

5. Papéis e Responsabilidades

Os seguintes papéis e responsabilidades se aplicam ao escopo desta Política.

5.1 Comitê de Tecnologia e Segurança da Informação

São funções do Comitê de Tecnologia e Segurança da Informação:

- Com anuência do Diretor Responsável, revisar e aprovar esta Política anualmente ou quando se fizer necessário para adequação a mudanças em normas regulatórias, leis, alterações de processos internos e externos, ambiente tecnológico, melhores práticas ou quaisquer outras demandas que este comitê definir.
- Promover a divulgação desta política a todos os Colaboradores, prestadores de serviços, fornecedores e parceiros de negócio que acessem sistemas ou informações da Empresa.
- Empreender ações, monitorar resultados das ações empreendidas, executar os planos de controles internos para mitigar riscos, com o objetivo de garantir a segurança das informações da Empresa.
- Cumprir e fazer cumprir os planos de ação decorrentes riscos de segurança, que exponham ou possam expor a Empresa a ocorrências de incidentes relacionados à segurança da informação.

5.2 Área de Segurança da Informação

Todos os Colaboradores da área de Segurança da Informação da Empresa devem:

- Propor continuamente melhorias nesta Política para o Comitê de Tecnologia e Segurança da Informação.
- Executar ações necessárias para que essa Política seja cumprida em sua integridade.
- Reportar ao Comitê de Tecnologia e Segurança da Informação sobre desvios na efetividade desta Política.

5.3 Usuários

Todos os Usuários da Empresa devem:

- Ter ciência desta Política e de seu papel na Segurança da Informação da Empresa.
- Cumprir as Políticas, diretrizes e procedimentos estabelecidos por esta Política e pelos documentos a ela associados;
- Participar ativamente para manter os ativos de informação da Empresa seguros.
- Utilizar os sistemas e serviços que acessem informações da Empresa somente para exercer suas funções e quando autorizado pelas áreas competentes.

- Notificar a área de Segurança da Informação sempre que encontrar desvios que ferem esta Política.

5.4 Proprietários

Proprietários são aqueles Colaboradores responsáveis pela manutenção, do ponto de vista dos processos de negócio da Empresa, de sistemas, de serviços ou de informações.

Os Proprietários devem:

- Autorizar o acesso aos recursos de sua responsabilidade somente aos Usuários que precisam delas para exercer suas funções profissionais e de maneira mais restritiva possível (por exemplo, somente leitura e limitado a uma visão, se isso for suficiente).
- Autorizar o acesso aos recursos de sua responsabilidade a outros sistemas ou serviços de maneira restritiva e na periodicidade que não afete a utilização do recurso original por seus Usuários.
- Efetuar as revisões de artefatos de sua responsabilidade na periodicidade definida nesta Política.

5.5 Gestores

Gestores são os Colaboradores com atribuições de gestão de pessoas, prestadores de serviços ou contratos.

Além dos papéis como Usuário, os Gestores devem:

- Garantir que a sua equipe siga e aplique esta Política.
- Gerir os acessos de sua equipe e de terceiros que estão sob sua responsabilidade, inclusive garantindo a exclusão dos acessos no caso de desligamento ou rescisão contratual.

6. Conceitos

6.1 Informação

Informação é todo ativo de conhecimento, registrado em suas diversas formas, impressa ou escrita em papel, armazenada eletronicamente, transmitida por meio físico ou por meios eletrônicos, apresentada em vídeos, gravações ou falada em conversas, derivado de dados da Empresa, de seus clientes e colaboradores ou de fontes externas que seja manipulada pelos seus Usuários para atingir seus objetivos de negócios.

A informação é um dos principais ativos de uma empresa e está relacionada à sua gestão estratégica, portanto deve ser adequadamente manuseada e protegida.

As informações manipuladas por processos e sistemas da Empresa, que tenham sido criadas ou mantidas nos seus bancos de dados ou estejam sob sua gestão são consideradas como de sua propriedade e não podem ser utilizadas para uso não profissional e sem sua autorização.

6.2 Segurança da Informação

A Segurança da Informação é obtida a partir da implementação de políticas, processos, procedimentos, e soluções tecnológicas. Os controles de Segurança da Informação devem ser definidos, implementados, monitorados, avaliados e melhorados continuamente.

Convém que isto seja feito em conjunto com outras condutas e processos de gestão, como:

- Cumprir com requisitos legais e regulatórios;
- Avaliar ameaças atuais e futuras ao negócio;
- Proteger informações sensíveis;
- Desenvolver sistemas e serviços com Segurança;
- Agir de maneira profissional e ética.

A Segurança da Informação se baseia nos seguintes pilares fundamentais:

- **Confidencialidade:** garante que a informação estará acessível apenas a pessoas autorizadas. A principal maneira de mantê-la assim é por meio de autenticação, controlando e restringindo o acesso, e impondo limitações de acesso aos dados sigilosos.
- **Integridade:** mede a exatidão da informação e seus métodos de modificação, manutenção e validade. Há perda de integridade quando a informação é alterada indevidamente ou quando não se pode garantir que a informação é a mais atualizada.
- **Disponibilidade:** garante que a informação esteja disponível sempre que for necessário para as pessoas autorizadas.
- **Autenticidade:** tem a finalidade de identificar e registrar o usuário que está realizando o envio ou modificação da informação, de modo que modificações de dados sejam devidamente documentadas.

- **Legalidade**: deve garantir que o uso de recursos de tecnologia e telecomunicação deve estar de acordo com as leis vigentes.

7. Privacidade e Investigação

Toda a informação manipulada por sistemas ou serviços da Empresa está passível de investigação, sem aviso prévio nas seguintes situações:

- A pedido da Diretoria da Empresa;
- A pedido da área de Compliance;
- A pedido dos gestores da empresa, desde que aprovado pela Segurança da Informação;
- Para investigação de suspeita de fraudes, de uso indevido ou não autorizado;
- Para atendimento de incidentes de segurança;
- Para atendimento de normas regulatórias;
- Para atendimento de obrigações legais.

A Empresa não garante a privacidade das informações pessoais dos colaboradores quando armazenadas em dispositivos corporativos e desestimula este tipo de uso dos seus recursos.

8. Propriedade Intelectual

Todas as informações, artefatos de tecnologia, artes e criações, planilhas, estratégias, documentos, textos ou outros produtos criados, adquiridos ou manipulados dentro das atividades profissionais dos Colaboradores da Empresa são de propriedade da Empresa e não podem ser copiadas, utilizadas para fins particulares ou enviadas para terceiros.

9. Criação, manipulação, uso e descarte

Toda informação ou ativo desenvolvido em ambiente corporativo deve ser utilizado para propósito do negócio, com uso correto e responsável.

A impressão de documentos contendo informações sensíveis deve ser evitada, mas se houver necessidade para atendimento das demandas profissionais, os documentos devem ser manipulados com acesso restrito.

Os documentos físicos e mídias eletrônicas devem ser descartados de forma segura, evitando a recuperação das informações durante o seu descarte, por exemplo, fragmentar papel e inutilizar mídias digitais fisicamente ou digitalmente com ferramentas apropriadas. Este procedimento inclui dispositivos de armazenamento (*hard disk*) de computadores em desativação.

10. Documentos físicos

Os documentos físicos podem ser digitalizados e, desta forma, substituir os originais. Os documentos físicos originais devem ser armazenados após a digitalização quando houver exigência específica das contrapartes ou de conforme regulação.

A substituição dos documentos impressos por digitalizados deve ser incentivada desde que as partes envolvidas acordem entre si, pois permite maior controle e segurança dos acessos às informações.

11. A retenção e o controle de acesso aos documentos físicos e aos documentos digitalizados devem obedecer aos mesmos critérios daqueles estabelecidos às informações originais.Classificação das informações

Toda informação criada e desenvolvida em ambiente corporativo deve ser classificada apropriadamente de acordo com sua confidencialidade, cabendo ao Gestor da área notificar e orientar seus colaboradores de suas responsabilidades.

As diretrizes para a classificação de informações estão descritas na Política de classificação das informações.

12. Proteção das informações

As informações classificadas como não públicas devem ser protegidas contra acessos indevidos (através de controle de acessos) e contra vazamento de dados.

13. Conscientização, sensibilização e treinamento de segurança

A área de Segurança da Informação deve estabelecer processos apropriados para disseminação da cultura de Segurança da Informação e Cibernética aos Usuários dos sistemas da Empresa que tenham acesso a informações sensíveis.

Os treinamentos e comunicação podem ser feitos de maneira presencial ou através de ferramentas de comunicação, como plataformas de treinamento online, portais, comunicações por e-mail e reuniões feitas por áudio ou vídeo conferência.

Todo novo Usuário deverá ser treinado com conceitos básicos de segurança de informação e, somente após o treinamento, será elegível aos acessos aos sistemas da empresa.

Os treinamentos de conceitos de segurança da informação devem ser aplicados ao menos anualmente ou conforme a necessidade específica de cada grupo.

Se algum Usuário for prestador de serviços terceirizado, o gestor de seu contrato pode solicitar à área de Segurança da Informação a dispensa dos treinamentos, desde que o nível de treinamento fornecido pela empresa ao Usuário for considerado suficiente.

14. Política de continuidade de negócios

A Política de continuidade de negócios visa eliminar ou minimizar os impactos no negócio de falhas de recursos humanos ou de componentes tecnológicos.

Ela é composta pelos seguintes itens:

- Análise de Impacto nos Negócios
- Plano de Continuidade de Negócios
- Plano de Recuperação de Desastre

O detalhamento dos componentes acima está na Política de continuidade de negócios.

14.1 Análise de Impacto nos Negócios (AIN)

O processo do Análise de Impacto nos Negócios (AIN) ou *Business Impact Analysis* (BIA) visa o mapeamento dos processos, atividades, sistemas e serviços críticos das áreas fundamentais para o negócio da Empresa. Sua função é identificar os Usuários, sistemas, serviços, tecnologias e outros recursos relevantes, que devem estar operacionais durante uma situação de contingência. A análise de impacto nos negócios influencia diretamente o Plano de Continuidade de Negócios e o Plano de Recuperação de Desastres.

14.2 Plano de Continuidade de Negócios (PCN)

O Plano de Continuidade de Negócios (PCN) ou *Business Continuity Plan* (BCP) é um conjunto de estratégias e planos de ações que contempla diversos cenários de indisponibilidade de recursos humanos, tecnológicos e físicos, visando garantir que os trabalhos e atividades essenciais da empresa sejam mantidas, assim como sua operacionalidade em um nível aceitável, até que se retorne à sua situação normal.

14.3 Plano de Recuperação de Desastres (PRD)

O Plano de Recuperação de Desastre (PRD) ou *Disaster Recovery Plan* (DRP) é um conjunto de estratégias e planos de ações que visam minimizar a indisponibilidade de serviços tecnológicos críticos para continuidade do negócio, mesmo após a ocorrência de incidentes que envolvam os datacenters ou a infraestrutura tecnológica e permite o restabelecimento das operações em tempo hábil e garante a realização das atividades críticas.

15. Resposta a incidentes críticos

Incidentes críticos são aqueles que afetam de maneira significativa a operação da Empresa ou a prestação de serviços aos Clientes.

Podem ocorrer no ambiente tecnológico da Empresa ou no ambiente do prestador de serviços em nuvem e devem ser notificados conforme descritos na Política de Gerenciamento de Incidentes.

O plano de resposta a incidentes críticos tem como objetivo minimizar o impacto do evento e garantir plano de ação para mitigação de novas ocorrências no futuro.

16. Resposta a incidentes de segurança da informação

Incidentes de segurança da informação são situações em que um ou mais ativos da informação da Empresa estão em risco, ou seja, algum evento confirmado ou sob suspeita relacionado a segurança dos sistemas, serviços ou componentes que suportam os ativos de informação da Empresa.

O plano de resposta a incidentes de segurança da informação tem como objetivo eliminar ou minimizar o impacto do evento. Para isso, os incidentes devem ser classificados por severidade e as várias áreas participantes devem ter seus papéis definidos para atuação na resolução, comunicação e registro do incidente.

O detalhamento deste plano está no Procedimento de Gerenciamento de Incidentes de Segurança.

17. Controle de acesso

17.1 Conceito

O controle de acesso tem como objetivo limitar o acesso a sistemas, serviços, informações e recursos somente àqueles necessários para execução das atividades profissionais de cada Usuário.

Os acessos aos recursos são liberados após registro de solicitação de acesso e sua respectiva aprovação por parte dos responsáveis, devendo respeitar os perfis definidos para cada função.

Os tipos de chamados para controle de acesso estão definidos no Catálogo de Serviços de Segurança da Informação.

17.2 Acessos aos recursos

Todos os Colaboradores receberão por padrão apenas os acessos básicos para acessar sua estação, a rede corporativa, o e-mail corporativo, navegação padrão na internet e seu local de trabalho, que são solicitados pelo departamento de Recursos Humanos da Empresa.

No caso de prestadores de serviços ou fornecedores, o acesso é solicitado pelo Gestor responsável pelo contrato.

Os demais acessos são solicitados através de chamados, que são submetidos à aprovação dos Gestores e dos Proprietários dos recursos.

Quando o sistema tiver uma Matriz de Segregação de Acessos, a liberação deve seguir o que está definido nesta. Exceções a esta regra devem ser aprovadas pela área de Compliance.

17.3 Entrada e saída de Usuários

A área de Recursos Humanos deve comunicar admissões e desligamentos de Colaboradores da Empresa à área de Segurança da Informação.

Os Gestores dos contratos devem comunicar contratação e rescisão de contratos de prestadores de serviço e fornecedores à área de Segurança da Informação.

A área de Segurança da Informação deve criar ou revogar os acessos necessários com a movimentação.

Os Gestores devem reter os recursos tecnológicos e o crachá de identificação do Usuário que está saindo. O crachá deve ser encaminhado para a área de Segurança da Informação e os demais recursos tecnológicos devem ser encaminhados para a área de Service Desk.

17.4 Transferência de área ou função

Havendo alteração de área ou função de Colaboradores, a área de Recursos Humanos deverá comunicar à área de Segurança da Informação para ajuste de perfis de acesso.

Havendo alteração contratual na prestação de serviços que mude o escopo de trabalho de um prestador de serviço ou fornecedor, o Gestor de contrato deverá comunicar à área de Segurança da Informação para ajuste de perfis de acesso.

A área de Segurança da Informação encaminhará ao Gestor do Usuário a lista dos atuais acessos, para que sejam feitos os ajustes necessários para adequação de perfil

de acesso à nova função do Usuário. Será necessário abertura de chamados para os novos acessos compatíveis com a nova função. Todos os acessos excedentes herdados da função antiga devem ser revogados.

17.5 Usuários e senhas de acesso

Os usuários e senhas de acesso corporativo são de uso individual, intransferível, cabendo ao seu titular total responsabilidade quanto a sua guarda. É proibido o compartilhamento de usuários e senhas de acesso.

As senhas, sempre que o sistema ou serviço permitir, devem seguir os seguintes parâmetros:

- tamanho mínimo: 6 (seis) caracteres;
- tempo máximo de expiração: 90 (noventa) dias;
- quantidade máxima de tentativas antes do bloqueio: 5 (cinco);
- duração do bloqueio: desbloqueio mediante avaliação do administrador;
- histórico mínimo de senhas utilizadas: 6 (seis);
- complexidade ativada: no mínimo, dois dos itens a seguir – letras maiúsculas e minúsculas, símbolos e números;
- armazenamento de forma criptografada;
- troca da senha padrão fornecida pelo fabricante do sistema operacional, do software de terceiros ou de sistemas.

Em caso de exceção ou limitação técnica do sistema ou serviço para composição e adequação dos parâmetros de senha de acordo com as regras acima, o risco deve ser analisado e validado por Segurança da Informação e, nos casos relacionados a sistemas de suporte a negociação, também por Compliance.

17.6 Múltiplo fator de autenticação

É obrigatório o uso do Múltiplo Fator de Autenticação (MFA) para os serviços e sistemas que tenham esta opção disponível e que manipulem informações confidenciais, sensíveis ou internas.

O MFA pode funcionar por SMS, token físico, aplicativo no smartphone, ligação telefônica ou leitura facial/biométrica e outros, dependendo das especificações técnicas de cada sistema ou serviço. Todas opções são aceitas, mas preferencialmente será utilizado o aplicativo no smartphone, por entregar maior nível de segurança e facilidade de implantação e manutenção.

Os casos de exceção ou limitação técnica do sistema ou serviço que impeçam a utilização do MFA deverão ser aprovados por Segurança da Informação e, nos casos relacionados a sistemas de suporte a negociação, também por Compliance.

17.7 Serviços de Acesso Remoto

O acesso remoto à rede corporativa será liberado somente para utilização de atividades relacionadas às atividades profissionais dos colaboradores. O acesso está autorizado para todos os diretores e Gestores.

Para demais Colaboradores que requeiram este acesso, deve haver aprovação do seu Gestor e da área de Recursos Humanos.

Para acesso de prestadores de serviços ou fornecedores, deve haver aprovação do Gestor do contrato e de Segurança da Informação.

Esse acesso poderá ser revisto e revogado a qualquer momento por determinação das áreas aprovadoras.

As equipes de Tecnologia e Segurança da Informação poderão, com a anuência do Usuário, efetuar acessos remotos às suas estações de trabalho para atendimento de incidentes, dúvidas ou solicitações.

A equipes de Segurança da Informação, Tecnologia e Compliance poderão acessar remotamente as estações dos Usuários no caso de investigação de incidentes de segurança, suspeita de vazamento, suspeita de fraudes ou riscos legais.

17.8 Acesso a redes sem fio

As redes sem fio (*wireless*) disponibilizadas na Empresa são segregadas da rede corporativa e podem ser usadas por Colaboradores, prestadores de serviço e clientes a critério dos Gestores.

Os recursos da rede wireless mesmo quando feitas por dispositivos pessoais não podem ser usados para navegação em páginas, serviços ou aplicativos que se utilizem de conteúdo inapropriado ou ilegal, nem para download de arquivos que infrinjam direitos de licença ou de uso.

A Empresa pode monitorar os sites acessados por seus Usuários sem qualquer aviso prévio e bloquear conteúdos que considera inapropriado. Havendo mau uso, poderá haver restrição de acessos.

17.9 Acesso Físico aos ambientes

Para algumas áreas da Empresa, é necessário implementar algum sistema de controle de acesso físico para restringir a entrada somente às pessoas autorizadas. O sistema de controle pode ser físico ou através de sistema automatizado, desde que sejam registrados os acessos ao ambiente. Devem ter acesso restrito:

- *Datacenter*: todas as instalações de processamento e guarda de informações deverão ser mantidas em áreas seguras e protegidas.
- Mesas de Operações: o acesso às Mesas de Operações deve ser controlado, não sendo permitida a presença de Clientes no ambiente.
- Administração de Carteiras: as atividades de administração de carteiras de valores mobiliários devem ficar em ambiente segregado das áreas que fazem intermediação e distribuição de valores mobiliários.

Havendo viabilidade técnica para implantação de circuito fechado de TV (CFTV) na localidade, deve-se posicionar câmera para gravação da circulação nos ambientes de acesso restrito.

17.10 Revisão de acessos

Anualmente, os Proprietários e Gestores devem revisar se os acessos concedidos aos Usuários estão de acordo com a necessidade atual da Empresa para cada recurso de sua responsabilidade. O resultado desta revisão resultará na manutenção, modificação ou remoção dos acessos concedidos aos Usuários.

Acessos com mais de 90 dias sem uso em qualquer sistema ou serviço podem ser desabilitados de acordo com a avaliação das áreas de Segurança da Informação e Tecnologia.

17.11 Matriz de segregação de acessos

Para os principais sistemas da Empresa, listados abaixo, é necessário o desenho da Matriz de segregação de acessos, que lista os perfis de acesso para cada área da Empresa que pode acessar o sistema:

- Sistemas que suportem os seguintes processos de negócio: Cadastro de Clientes, *Suitability*, Executar Ordens, Liquidar Negócios, Administrar Custódia de Ativos e Posições e Gerenciar Riscos. Incluir nesse inventário os sistemas de negociação e de roteamento de ordens – OMS.

As matrizes de segregação de acessos devem atender aos princípios de segregação das atividades entre os Usuários de forma a evitar conflito de interesses na execução de suas atividades.

As matrizes são criadas com base na análise do Proprietário do sistema, responsável em determinar quais acessos são necessários para cada área e devem ser aprovadas pela área de Compliance.

18. Recursos de armazenamento de dados

Os Usuários receberão acesso aos recursos de armazenamento de dados necessários para desenvolvimento de suas funções, havendo previa análise e autorização do Gestor e/ou Proprietário.

As seguintes restrições se aplicam a armazenamentos de dados:

- É proibida a guarda de arquivos não autorizados como executáveis, arquivos de áudio e vídeo não relacionados à atividade do usuário, ou quaisquer outros arquivos sem licença, direito de uso ou obtidos por fontes não autorizadas.
- É proibido efetuar copias das informações da instituição, seja por *pen drive*, e-mail, serviços de armazenamento em nuvem, ferramentas colaborativas e redes sociais, a não ser que autorizado pelo Gestor e pelo Proprietário e comunicado à Segurança da Informação.
- Não é permitido armazenar documentos corporativos no disco local das máquinas, os quais não possuem rotina de *backup*. A eventual perda de informações armazenadas neste local é de total responsabilidade do Usuário.
- É proibido o uso de dispositivos de armazenamento externo, como *pen drives* e discos externos para cópias de arquivos de propriedade da Empresa, mesmo que seja para cópia de segurança (*backup*).
- Exceções deverão ser autorizadas pela área de Segurança da Informação.

19. Utilização de correio eletrônico

O serviço de correio eletrônico, disponibilizado através do e-mail corporativo, deve ser utilizado apenas para fins profissionais. As informações das mensagens recebidas e enviadas são de propriedade da Empresa e podem ser monitoradas continuamente e sem aviso prévio para fins de segurança da informação e Compliance.

É proibido enviar informações internas, sensíveis ou confidenciais da Empresa para destinatários não autorizados a manipular tais informações, sejam eles internos ou externos.

Estão vetadas práticas abusivas tais como: a circulação de spam ou correntes, conteúdo discriminatório, com mensagens de viés político, conteúdo restrito ou ilegal, entre outros. Nos casos avaliados como inapropriados, caberão sanções administrativas.

Caso um Usuário receba uma mensagem com informações que não deveria ter acesso, ou seja, que foi enviada por erro do remetente, deve apagar imediatamente e comunicar à área de Segurança da Informação.

É esperado o uso adequado por todos os Usuários, evitando-se mensagens com números excessivos de destinatários, buscando-se objetividade.

A utilização de serviços de e-mails não corporativos (Gmail, Yahoo, Outlook pessoal etc.) é proibida devido à facilidade no extravio de informações corporativas e à impossibilidade de monitoração. Exceções devem ser avaliadas pela área de Segurança da Informação e Compliance.

20. Utilização e aquisição de sistemas e softwares

Todos os sistemas, serviços e softwares utilizados pelo colaborador deverão ser aprovados e homologados pela Empresa, através das áreas de Infraestrutura, Desenvolvimento e Segurança da Informação.

Além da homologação das áreas acima, alguns sistemas e serviços deverão ser aprovados também por Compliance:

- Aqueles que efetuam atualizações no Cadastro e *Suitability* de Clientes;
- Aqueles que transmitam ou executem Ordens de intermediação de valores mobiliários;
- Aqueles relacionados à administração de carteiras de valores mobiliários.

Todos os sistemas, serviços e softwares instalados ou em uso na empresa devem possuir licenças de uso adequadas à sua utilização, número de usuários, número de servidores ou qualquer outra métrica de cobrança.

Não é permitido instalar nenhum software não homologado, mesmo que seja livre de custos de licenciamento, pois isso pode causar problemas no ambiente operacional da empresa.

As ferramentas e serviços autorizados estão na Lista de ferramentas e serviços homologados.

21. Sistemas de Mensagens Instantâneas

O sistema de mensagens instantâneas destina-se para fins corporativos e suas mensagens são de propriedade da Empresa, podendo ser monitoradas sem aviso prévio. Será liberado o uso somente dos sistemas homologados e para aqueles funcionários que assim necessitem para o desempenho de suas tarefas. As mensagens devem se limitar a questões inerentes à sua função profissional.

A utilização das ferramentas destinadas ao registro de ordens de clientes deve se limitar às ferramentas homologadas pela Empresa e que forneçam nível de rastreabilidade exigida por órgãos reguladores e nível de segurança adequado.

É proibido enviar, através de sistemas de mensagens instantâneas, informações internas, sensíveis ou confidenciais da Empresa para destinatários não autorizados a manipular tais informações, sejam eles internos ou externos.

22. Navegação na internet

O uso da Internet deve ser limitado a páginas relacionadas à sua função desempenhada na Empresa.

É permitida a utilização de sistemas e serviços em nuvem que utilizam de navegação na internet, desde que homologados.

O log de navegação na internet pode ser monitorado sem qualquer aviso prévio, podendo haver bloqueio de conteúdos inapropriados.

23. Ambiente de trabalho seguro

Visando manter nosso ambiente de trabalho seguro, deve-se:

- Bloquear o computador sempre que sair da mesa.
- Manter as mesas de trabalho, corredores e salas de reunião limpas e organizadas, inclusive livres de papeis, livros, blocos de notas, ferramentas, *post-its*, cadernos e caixas.
- Conservar as mesas, cadeiras, computadores, telefones e demais equipamentos e notificar o gestor quando encontrar algum objeto danificado.
- Retirar as folhas impressas da impressora imediatamente após sua impressão, para evitar que informações sejam acessadas por pessoas não autorizadas.

- Guardar objetos que não sejam utilizados no dia a dia em depósitos ou locais apropriados.
- Evitar deixar objetos de valor nas mesas, sejam da empresa ou pessoais.

É proibido tirar fotos, gravar ou filmar áreas da Empresa sem autorização do Gestor da área. Fotos ou filmagens que mostrem quadros, telas ou cartazes com informações internas são proibidas. Fotos que permitem identificação do local só podem ser tiradas com autorização das áreas de Segurança da Informação e Marketing.

É proibido, em qualquer circunstância, filmar, gravar ou fotografar os ambientes das Mesas de Operações.

24. Criptografia de dados

A criptografia é um processo de transformação de dados de forma que eles não tenham mais o formato original e, desta forma, não possam ser lidos sem que se tenha acesso uma chave de descriptografia. Pode ser implementada através de diversos algoritmos, por sistemas, software ou hardware.

É recomendada a utilização da criptografia sempre que há manipulação de informações confidenciais. Entretanto, o processo de criptografia e descriptografia muitas vezes é complexo para os sistemas e serviços que não estejam preparados para sua implementação.

Devem implementar criptografia os seguintes componentes:

- Comunicação de informações sensíveis pela internet;
- Armazenamento de senhas nos bancos de dados;
- Transmissão de usuários e senhas pela rede interna;
- Transferência de arquivos com ambientes externos;
- Dispositivos de armazenamento de computadores portáteis;
- Serviços de cofres de senhas.

25. Recursos de Tecnologia da Informação

A utilização de algumas disciplinas de tecnologia da informação afeta o nível de segurança do ambiente. Para estas, estão abaixo descritos os requisitos mínimos para sua operação.

25.1 Gestão de ativos

É desejável ter o inventário de ativos de todos os sistemas e serviços da Empresa através de software(s) apropriado para este fim.

É obrigatório ter inventário de sistemas e ativos que suportam os seguintes processos de negócio: Cadastro de Clientes, *Suitability*, Executar Ordens, Liquidar Negócios, Administrar Custódia de Ativos e Posições e Gerenciar Riscos. Incluir nesse inventário os sistemas de negociação e de roteamento de ordens – OMS.

Os componentes da infraestrutura devem ser atualizados periodicamente com atualizações de segurança, conforme orientação dos fornecedores.

25.2 Segurança de redes

Para segurança de redes devem ser implementadas ferramentas de *firewall* para controlar fluxos de dados nas redes internas, externas e internet.

Devem ser implantados controles para segregação das redes de produção das redes de desenvolvimento e homologação.

Devem sem implantados controles para segregação das redes de dispositivos (estações de trabalho, dispositivos móveis ou *desktops* virtuais) das redes de produção, homologação e desenvolvimento.

Para liberação de regras de acesso, deve-se seguir o Procedimento para liberação de regras de *firewall.*

25.3 Operação de recursos computacionais

Os recursos computacionais (servidores, serviços corporativos e dispositivos de rede) devem ser operados por equipe especializada. Os usuários devem ser nominais ou identificáveis através de trilhas de auditoria habilitada para os servidores de produção.

Os componentes que permitirem a instalação de software antivírus, como servidores, devem tê-lo instalado e ativo.

Devem ser executados testes periódicos e varreduras para detecção de vulnerabilidades no ambiente.

25.4 Gestão de estações de trabalho

As estações de trabalho dos Usuários da Empresa devem ser administradas por equipe especializada, seguindo as melhores práticas de mercado para esta prática.

- Devem possuir software de antivírus instalado e ativo.
- Devem ser atualizadas periodicamente com atualizações de segurança, conforme orientação dos fornecedores.

25.5 Monitoração

A monitoração de diversos itens de configuração da infraestrutura da Empresa deve ser periodicamente analisada e, caso haja algum incidente, deve ser registrado e tratado conforme a Política de Gerenciamento de Incidentes.

25.5.1 Infraestrutura de TI

Deve haver monitoração preventiva da disponibilidade, da capacidade e do desempenho (processador, disco rígido e memória RAM) dos servidores do ambiente produtivo, incluindo todos os canais de comunicação utilizados pelo Participante, como: *links* de comunicação com a B3 (RCB/RCCF) e links de comunicação entre localidades do Participante (*lan-to-lan*).

25.5.2 Acessos a bancos de dados

Os acessos a bancos de dados feitos por terceiros devem ser monitorados através de:

- Trilha de auditoria, que pode ser habilitada com filtros de usuários, tabelas e transações com o objetivo de diminuir o impacto na performance e reduzir o espaço em disco utilizado pelo banco de dados. A monitoração da atividade de consulta ("*select*") na base de dados também é necessária, pois permite que a base inteira de cliente seja coletada.
- Ferramenta que permita gravação de vídeo ou capturas de tela ("*printscreen*"): gravação da tela com a sessão de conexão ao banco de dados pode ser gravada para evidenciar as ações executadas pelo fornecedor no período de acesso.
- Manutenção assistida: um Colaborador da Empresa acompanha as atividades realizadas durante o período de acesso.

As trilhas acima devem permitir identificar o usuário, data, horário e evento efetuado no banco de dados (alteração, inclusão ou exclusão).

25.5.3 Monitoramento da Segurança da Rede

Deve ser implementada auditoria para identificar tentativas de acessos indevidos aos dispositivos de rede (no mínimo, aos *firewalls*), incluindo informações necessárias para buscar a identificação do Usuário ou serviço infrator.

25.5.4 Rotinas de *backup*

Deve-se monitorar as rotinas de *backup* para validação de sua execução nos dias em que houver movimento de negócio que sensibilizem os dados (dias úteis).

25.6 Cópias de segurança ou *backup*

Devem ser armazenados cópias de segurança das informações armazenadas em bancos de dados, servidores e outros serviços para recuperação em caso de incidentes.

Os requisitos para cópias de segurança das informações estão detalhados na Política de cópias de segurança de informações.

25.7 *Datacenter*

Deve haver ao menos um *datacenter* para ambiente de produção e um segundo para ambiente de contingência, sendo que estes não podem ficar no mesmo endereço físico.

Os *datacenters* que armazenam os ambientes de produção e contingência devem possuir certificado de segurança reconhecido, como: SAS70, ISAE 3402, TIER ou equivalentes.

Os sistemas e serviços críticos devem ser replicados do(s) *datacenter*(s) de produção para o(s) *datacenter*(s) de contingência, conforme os requisitos de disponibilidade exigidos pelo negócio.

26. Contratação de serviços de computação em nuvem

Quando houver necessidade de contratação de serviços em nuvem, as áreas de Tecnologia e Segurança de Informação devem ser envolvidas para avaliação de aderência aos requisitos abaixo, de acordo com a criticidade das informações processadas ou armazenadas:

- Análise da capacidade de processamento.
- Avaliação das formas de acesso às informações processadas ou armazenadas pelo prestador de serviço.
- A garantia da confidencialidade, a integridade, a disponibilidade e a recuperação dos dados e das informações processados ou armazenados pelo prestador de serviço.
- Avaliação de recursos de gestão e monitoração.
- A segregação dos dados da Empresa dos dados dos demais clientes do fornecedor.

O detalhamento dos requisitos encontra-se no Procedimento para avaliação e contratação de serviços na nuvem.

27. Utilização de dispositivo pessoal

Os Usuários que optarem por usar seu dispositivo pessoal para fins profissionais deve obter autorização, conforme descrito na Política de utilização de dispositivo pessoal. Neste caso, deve seguir as regras da Empresa para adequar seu dispositivo aos padrões de segurança definidos pela Empresa de forma a não aumentar os riscos de segurança.

28. Gerenciamento de riscos de segurança

Um risco de segurança é um evento futuro que pode ocorrer e causar impacto negativo num ativo de informação da Empresa.

Os riscos devem ser avaliados conforme seu impacto ao negócio e probabilidade de ocorrência e apresentados para o Comitê de Tecnologia e Segurança da Informação através da Matriz de riscos de Segurança da Informação. Os riscos prioritários devem ser tratados e aqueles que forem avaliados como aceitáveis para o negócio, devem passar pelo processo de aceitação de riscos. Os projetos que implementem planos de ação para mitigação de riscos devem estar listados nos Projetos de Segurança da Informação.

Este processo está detalhado no Procedimento de Gestão de Riscos de Segurança da Informação.

29. Testes de segurança

Alguns testes de segurança são necessários para avaliar se o nível de segurança dos componentes humanos e tecnológicos estão em níveis adequados.

Devem ser realizados, ao menos anualmente, os seguintes tipos de testes:

- Testes de invasão (*pentests*): são testes que buscam simular uma invasão para detectar vulnerabilidades na aplicação ou na infraestrutura.
- Testes para avaliação do nível de conscientização de Usuários: testes aplicados para avaliar a efetividade dos treinamentos aplicados nos Usuários, como avaliações ou simulação de *phishing*.

- Testes de análise de varredura para detecção de vulnerabilidades: testes para avaliação de sistemas operacionais e softwares básicos, como virtualizadores, servidores web, servidores de aplicação, controladores de filas e outros.
- Testes do Plano de Continuidade de Negócio: testes de cenários de desastre para avaliação do PCN.

Devem ser realizados, ao menos a cada bimestralmente, o seguinte tipo de teste:

- Testes de restauração de cópias de segurança de informações: testes para avaliação da efetividade dos procedimentos de *backup*.

Os resultados dos testes, assim como os respectivos planos de ação para as fragilidades apresentadas devem ser apresentados ao Comitê de Tecnologia e Segurança da Informação dentro do ano calendário de referência para conhecimento e priorização.