Política de Segurança da Informação e Cibernética

v.1.4.2 - Março 2024

Resumo

Estabelecer normas de utilização a serem adotadas por todos os colaboradores, prestadores de serviços, colaboradores, fornecedores e/ou parceiros referente à Política de Segurança Cibernética e da Informação (PSCI), tendo como objetivo proteger os ativos de informação e formar a base para o estabelecimento de todas as normas e procedimentos a serem seguidos para garantir o fluxo de informações adequado.

XMS INVESTIMENTOS

Tabela de Versões:

Versão	Data	Descrição
v.1.0.0	março/2011	Documento Original
v.1.1.0	abril/2016	Inclusão de normas e procedimentos de segurança cibernética / alteração título política
v.1.1.1	agosto/2020	Revisão Geral, Padronização Gráfica e Inclusão de Assinaturas
v.1.3.0	setembro/2020	Revisão, Inclusão Conteúdo: Matriz de Riscos Supervisão e Plano de Resposta a Incidentes.
v.1.3.1	outubro/2020	Inclusão de vedação à utilização de Smartphones nas estações de trabalho. Exclusão de Normas de Sistema Antivírus. Adequação Geral de Conteúdo.
v.1.4.1	Agosto/2022	Inclusão da referência ao cumprimento da Lei Geral de Proteção de Dados Pessoais (LGPD)
v.1.4.2	Março/2024	Atualização de Nomes de Pastas e Arquivos. Revisão geral, padronização gráfica e atualização de nomes e nomenclaturas.

Validade: Indeterminado, com prazo de atualização não superior a 24 meses desde a última versão.

Área Responsável: Compliance

Aplicação: XMS Investimentos

Conteúdo do Documento

Este documento aborda as estratégias de segurança da empresa e abrangerá os seguintes aspectos:

Áreas de Aplicação

Todas as áreas da empresa bem como prestadores de serviço, fornecedores, parceiros e sistemas de ambientes de informática, como: redes locais, intranet, internet, extranet e a outras informações geradas, mantidas e/ou disponíveis em outros meios que não os eletrônicos. Destacamos três tipos de participantes nesta política:

- Usuário - pessoa que interage diretamente com o sistema computadorizado.
- Gestores de área - responsáveis pela administração e gestão da empresa.
- Terceiros – prestadores de serviço ou parceiros com acesso à informações.

Todos os gestores de área, colaboradores, estagiários, prestadores de serviço, fornecedores e/ou parceiros devem observar e atender a todas as normas que regulamentam as atividades da Instituição.

Diretrizes, Princípios e Conceitos

Informação

A informação é um dos ativos mais importantes para os negócios da organização e consequentemente necessita ser adequadamente protegida. No caso de informações privilegiadas detidas sobre posição de clientes e de relatórios e estudos próprios sobre títulos e valores mobiliários que possam prejudicar o desempenho das carteiras, deve-se ter especial atenção. Manter a confidencialidade, integridade e disponibilidade da informação são essenciais para preservar a competitividade, faturamento, lucratividade, atendimento dos requisitos legais e a imagem da empresa no mercado. A informação pode existir em muitas formas. Ela pode ser impressa ou escrita em papel, armazenada eletronicamente, transmitida pelo correio ou através de meios eletrônicos, mostrada em filmes ou falada em conversas. Seja qual for a forma apresentada ou o meio através do qual a informação é compartilhada ou armazenada, é recomendado que ela seja sempre protegida adequadamente.

Segurança da Informação / Cibernética

Todas as informações devem ser protegidas contra acesso, modificação, destruição, ou divulgação não autorizada, independentemente do meio em que se encontrem. A informação é um dos ativos mais importantes para os negócios da organização e consequentemente necessita ser adequadamente protegida. Manter a confidencialidade, integridade e disponibilidade da informação são essenciais para preservar a competitividade, faturamento, lucratividade, atendimento dos requisitos legais e a imagem da empresa no mercado. A informação pode existir em muitas formas. Ela pode ser impressa ou escrita em papel, armazenada eletronicamente, transmitida pelo correio ou através de meios eletrônicos, mostrada em filmes ou falada em conversas. Seja qual for a forma apresentada ou o meio através do qual a informação é compartilhada ou armazenada, é recomendado que ela seja sempre protegida adequadamente.

A segurança das informações geralmente é associada aos sistemas informatizados, mas não se limitando aos mesmos, e é frequentemente colocada à prova por diversos tipos de ameaças, tais como: fraudes eletrônicas, vírus, hackers, espionagem, sabotagem, ou engenharia social, por exemplo.

O conceito básico de segurança é a proteção dada às informações contra diversos tipos de ameaças para preservá-las de ações não autorizadas ou mal intencionadas, garantindo a continuidade dos negócios e minimizar os danos aos negócios em situação de risco. Isso sempre deve ser feito observando-se os riscos envolvidos, a tecnologia e o custo de implementação dos mecanismos de controle, proteção e recuperação necessários.

Princípios de Segurança

- **Confidencialidade** - a garantia de que a informação é acessível somente a pessoas autorizadas a terem acesso, condição essencial para preservar as informações, reduzindo as ameaças de ações não autorizadas ou atos mal-intencionados de terceiros. Este princípio é abordado pela **Política de Segurança**.
- **Integridade** - Garantia de exatidão da informação e métodos de processamento.
- **Disponibilidade** - Garante que os usuários autorizados obtenham acesso à informação sempre que necessário.
- **Irretratabilidade** - Visa garantir que o autor não negue ter criado e assinado o documento.
- **Autenticidade** - Garantia da identidade de quem gerou a informação.
- **Legalidade** - Atende a legislação vigente quanto à guarda e ao sigilo das informações.

A segurança das informações é alcançada por meio de instrumentos adequados de controles, como políticas, práticas, normas, procedimentos, softwares e estrutura organizacional, sendo que estes precisam ser estabelecidos para garantir que as normas dessa política sejam cumpridas.

Matriz de Riscos (Informações Críticas)

Para a definição da Matriz de informações críticas, utilizamos os sistemas de arquivos de nosso leiaute de infraestrutura tecnologia, que também está presente em nossa **Política de Segregação de Atividades**. O sistema de arquivos está dividido no servidor em três grandes grupos: arquivos confidenciais, arquivos de trabalho e arquivos de dados, sendo este último utilizado para alimentar informações para uso no trabalho cotidiano da empresa. Dentro de cada grande grupo, foram divididas as seguintes pastas de dados, conforme a tabela abaixo:

Grupo	Pastas	Áreas de Acesso Exclusivo

Arquivos Confidenciais	Financeiro Admin	Administradores
Arquivos de Trabalho	Gestão - Investimentos Compliance e Riscos Expansão	Equipe Investimentos Equipe Adm. Controles e Riscos Equipe Adm. Controles e Riscos Equipe Adm. Controles e Riscos
Arquivos de Bases de Dados e Outros	Geral - Dados	Equipe Investimentos e Adm. Controles e Riscos
Arquivos de Acesso Comum	Geral - Políticas e Geral	Todos

Desta forma, a classificação por nível de risco é descrita na tabela abaixo:

Grupo	**Nível de Risco**	**Áreas de Acesso Exclusivo**
Arquivos Confidenciais	Baixo	Os arquivos Confidenciais são acessados somente por diretores da XMS Investimentos
Arquivos de Trabalho	Médio	Os arquivos de Trabalho são acessados somente pela Equipe Correspondente a cada Pasta de Trabalho.
Arquivos de Bases de Dados e Outros	Baixo	Arquivos de Base Pública
Arquivos de Acesso Comum	Baixo	Arquivos Não Confidenciais

Descrição dos mecanismos de supervisão de riscos

A área de compliance utiliza o G Suíte para registros de auditoria em todos os sistemas de arquivos da XMS Investimentos. Através desses relatórios, temos o controle do evento, nomes dos arquivos, usuários, códigos dos itens, visibilidade (se compartilhado externamente) e o endereço de IP utilizado. Para os arquivos que fazem parte dos

grupos de Risco Médio, o acompanhamento é feito constantemente através de Alertas por Usuário, sob responsabilidade da Área de Compliance.

Plano de Resposta da Incidentes

Para incidentes, deve-se formar um Grupo de Trabalho (que também é criado em situações contingenciais, conforme o **Plano de Continuidade de Negócios** da instituição, sendo as suas principais atribuições:

- Receber informações sobre situações que possam afetar o funcionamento da Gestão;
- Avaliar a criticidade e determinar providências para iniciar operações em situação de contingência;
- Acompanhar as providências de correção das falhas;
- Determinar o fim da contingência e acompanhar as providências de recuperação para o retorno à normalidade;
- Elaborar e fazer cumprir o calendário de treinamento e testes;
- Avaliar o resultado das ações de contingência, propondo correções e melhorias; e
- Recomendar a contratação da prestação de serviços e processos para atendimento da Contingência.

Assim que deflagrar a contingência o GT comunicará às pessoas chaves envolvidas que, por sua vez, avisarão os demais participantes das ações previstas e previamente conhecidas. As pessoas envolvidas terão em seu poder uma relação com nome e telefones (residencial, celular e alternativo) e, conforme previamente estabelecido, entrarão em contato com seus pares para agilizar o processo. Tais pessoas serão informadas da situação e da ação de contingência adotada pelo GT, com procedimentos a serem definidos pelo grupo. O fim da contingência também é informado aos envolvidos.

Normas Gerais

Normas de Rede e Sistemas

O controle de acesso lógico ou à rede e sistemas deve ser feito para proteção dos dados contra problemas de segurança relacionados à quebra de confidencialidade e integridade, cuja finalidade é garantir que apenas usuários e processos autorizados tenham acesso a determinadas informações e que possam executar apenas as ações previamente definidas.

No contexto de segurança de rede, o controle de acesso é a habilidade de limitar ou controlar o acesso aos computadores hospedeiros ou aplicações através dos enlaces de comunicação e do controle de acesso físico. Para tal, cada entidade que precisa obter acesso ao recurso deve primeiramente ser identificada, ou autenticada e de forma a que os direitos e permissões de acesso sejam atribuídos ao usuário.

O Controle de Acesso Lógico permite que os sistemas de TI verifiquem a identidade dos usuários que tentam utilizar seus serviços. Como exemplo mais comum, temos o *login*

de um usuário em um computador. O processo realizado é o de identificação e autenticação deste usuário.

A autenticação é o processo no qual ele aponta cada usuário, geralmente através do uso de uma senha.

Procedimentos formais devem ser conduzidos para gerenciar o acesso à informação, como:

- Registro de novos usuários;
- Gerenciamento de senhas de usuários;
- Reavaliações ou revogação de acesso.

Os componentes de identificação do usuário e senha são de uso pessoal e exclusivo do titular. Qualquer acesso a aplicações deve ser precedido de autenticação e controle de acesso a recursos, de modo a permitir rastreamento das operações realizadas.

Qualquer alteração na configuração física ou lógica dos recursos de tecnologia deve ser feita por pessoal especializado e autorizado pela empresa.

Todas as conexões da rede interna da empresa com redes externas devem operar por meio de implementações seguras e monitoradas (com roteadores e *firewalls*) e a geração de eventos de segurança (log) deve estar sempre ativa a ser periodicamente analisada.

Controles de proteção física, de acesso lógico, contra vírus e backup de dados devem ser estabelecidos quando se utilizam recursos de computação móvel (ex. notebooks)

Por padrão todos os novos colaboradores da instituição deverão ter acesso aos seguintes sistemas:

- Sistema operacional (*login* de rede)
- Acesso à rede (pastas correspondentes a sua função)
- E-mail corporativo, acesso à caixa postal para envio e recebimento de mensagens

No caso de desligamento serão bloqueados todos os acessos aos sistemas/rede do colaborador.

Caso o funcionário desligado necessite de arquivos pessoais armazenados na sua máquina ou na rede, os responsáveis farão o procedimento com ele.

Regras de Autenticação

- Os usuários deverão trocar as senhas em intervalos que não excedam o limite de 180 (cento e oitenta) dias.
- Deverá ter o tamanho mínimo de 6 (seis) caracteres e, no máximo 10 (dez) caracteres, conforme a extensão da aplicação ou do sistema.
- Invocação automática de timeout e nova autenticação do usuário depois de um período de inatividade do terminal de 15 (quinze) minutos.

- O acesso do usuário será suspenso após 3 (três) tentativas inválidas, no máximo, e o desbloqueio deverá ser efetuado pelo administrador.
- As senhas devem ser mantidas de forma criptografada e, quando possível, transmitidas tecnicamente por meio de criptografia.

Regras para Uso de Pastas de Rede

- Usuários que possuírem acesso à rede deverão acessar as pastas de acordo com as suas atividades ou a área a qual está alocado.
- Os colaboradores da instituição bem como prestadores de serviço/fornecedores que possuírem acesso aos diretórios não poderão, em qualquer tempo ou sob qualquer propósito, apropriar-se das informações (cópia).
- É proibido o armazenamento de arquivos dos tipos: e-mail (.pst), áudio, vídeo, fotos e executáveis nos diretórios da rede bem como nas estações de trabalho da instituição.
- Colaboradores que necessitarem trabalhar com arquivos de áudio, vídeo, fotos e executáveis nos diretórios da rede ou nas estações de trabalho da instituição devem ter autorização dos sócios-gerentes da empresa.

Normas de Utilização da Internet

- O uso da internet deve ser exclusivo para finalidades e propósitos aprovados pela instituição e sendo esse de interesse dela.
- A empresa, a qualquer momento, poderá rastrear e monitorar os itens acessados por qualquer pessoa sem aviso prévio.
- Todos são responsáveis pelas ações realizadas por meio do seu acesso à internet.
- Não é permitida a navegação em sites de jogos, sexo, chats (bate-papo), webmail (UOL, Yahoo, terra, gmail etc.), redes sociais (Facebook, Instagram etc.) ou qualquer site de entidades ou facções que preguem qualquer tipo de discriminação ou incentivo à violência.
- Não é permitido baixar arquivos (download) contendo imagens ou textos pornográficos, abusivos, racistas, constrangedores ou quaisquer outras informações que possam denegrir a imagem da instituição.
- Todos os usuários são responsáveis por proteger os equipamentos da ação de vírus e outros tipos de programas maliciosos que são propagados pela internet e que possam causar danos à instituição.
- Não é permitido realizar ações de invasão (hacker) de sistemas de informação de quaisquer companhias ou entidades ou ainda se passar por “hacker” com o intuito de acessar sem autorização os sistemas de informação da instituição.

Responsabilidade e forma de uso

- O usuário é responsável por todo acesso realizado com a sua autenticação.
- O usuário é proibido de acessar endereços de internet (sites) que:
- Possam violar direitos de autor, marcas, licenças de programas (softwares) ou patentes existentes.
- Possuam conteúdo pornográfico, relacionado a sexo, exploração infantil ou ao crime de pedofilia.
- Contenham informações que não colaborem para o alcance dos objetivos da XMS Investimentos.

- Defendam atividades ilegais. Menosprezem, depreciem ou incitem o preconceito a determinadas classes como sexo, raça, orientação sexual, religião, nacionalidade, local de nascimento ou deficiência física.
- O usuário deve garantir que está cumprindo a legislação em relação ao direito autoral, licença de uso e patentes existentes e que o uso do material foi autorizado pelo gestor da sua área.

Uso de serviço de rádio, TV, download de vídeos, filmes e músicas.

- É proibido o uso de serviços de rádio, TV, download de vídeos, filmes e músicas, através dos computadores da XMS Investimentos, exceto em eventuais situações de uso profissional autorizado pelo gestor da área e pela área de infraestrutura.

Uso de Correio Eletrônico particular tipo Webmail

- É proibido o acesso aos serviços de correio eletrônico particular, tipo Webmail, através dos recursos de tecnologia da XMS Investimentos.

Normas de Utilização de Correio

- O uso do correio eletrônico deve ser exclusivo para atividades relacionadas ao negócio da empresa.
- Somente deve ser utilizado software homologado pela instituição para a utilização do correio eletrônico.
- Cada usuário é responsável pela sua conta de correio eletrônico e o mesmo não deve ser compartilhado.
- As senhas de arquivos anexados devem ser transmitidas por outro meio de comunicação que não o e-mail com o objetivo de garantir o seu sigilo. Toda mensagem criada e armazenada nos computadores da empresa é de propriedade dela.
- A instituição reserva-se ao direito de acessar os correios eletrônicos.

Responsabilidades e forma de uso

O usuário que utiliza um endereço de correio eletrônico:

- É responsável por todo acesso, conteúdo de mensagens e uso relativos ao seu e-mail.
- Pode enviar mensagens necessárias para o seu desempenho profissional na empresa.

É proibido criar, copiar ou encaminhar mensagens ou imagens que:

- Contenham declarações difamatórias ou linguagem ofensiva de qualquer natureza.
- Façam parte de correntes de mensagens, independentemente de serem legais ou ilegais.
- Repassem propagandas ou mensagens de alerta sobre qualquer assunto. Havendo situações em que o usuário ache benéfico divulgar o assunto para a Empresa, a sugestão deve ser encaminhada para a Área de Recursos Humanos, que definirá a sua publicação ou não.

- Menosprezem, depreciem ou incitem o preconceito a determinadas classes, como sexo, raça, orientação sexual, idade, religião, nacionalidade, local de nascimento ou deficiência física.
- Possuam informação pornográfica, obscena ou imprópria para um ambiente profissional.
- Sejam susceptíveis de causar qualquer tipo de prejuízo a terceiros.
- Defendam ou possibilitem a realização de atividades ilegais.
- Sejam ou sugiram a formação ou divulgação de correntes de mensagens.
- Possam prejudicar a imagem da XMS Investimentos.
- Sejam incoerentes com o nosso Código de Ética.

Normas de Mensagens Instantâneas

- A utilização do sistema de mensagens instantâneas será restrita às áreas de mesa de operações e atividades relacionadas; áreas que envolvam contato com o cliente, e diretoria; sendo proibido o uso desses ou de qualquer sistema que proporcione a troca de mensagens instantâneas por outras áreas da instituição.
- As mensagens trocadas através de *Google Chats* serão gravadas e armazenadas, havendo possibilidade de serem auditadas e qualquer momento.
- É terminantemente proibido:
    - A utilização do *Google Chats* para fins pessoais;
    - A transmissão de qualquer anexo via *Google Chats*;
    - Troca de mensagens instantâneas através do uso de webmails, exemplo via WhatsApp, Telegram, hotmail.com, gmail.com ou outros.

Normas de Utilização de Software

- Todos os softwares e programas utilizados na instituição devem ser aprovados por ela, devendo esses ser devidamente licenciados e compatíveis com os sistemas em uso.
- Não é permitida aos usuários a instalação de nenhum tipo de software, seja licenciado ou não, que não os previamente estabelecidos pela instituição.
- Todos os computadores da instituição devem possuir softwares antivírus ativos devidamente configurados e atualizados de acordo com as normas da área de tecnologia.
- Não é permitida aos usuários a posse, cópia ou distribuição de arquivos que possuam proteção de direitos autorais e/ou de propriedade intelectual, tais como arquivos de música, vídeo, imagens, áudio e textos.

Normas de Utilização de Hardware e Smartphones

- É vedada a utilização de smartphones ou telefones pessoais nas áreas de trabalho, salvo por áreas que utilizem deste equipamento para fins profissionais.
- Todo hardware deve ser avaliado e aprovado por decisão dos gestores de área. A aprovação se dará após avaliação e confirmação de necessidade de uso do equipamento.
- Todos os usuários são responsáveis pela utilização de seus equipamentos.
- Todos os equipamentos de computação da instituição devem possuir identificação conforme definido por ele.

- Toda manutenção de equipamentos de computação da instituição deve possuir mecanismos para evitar acesso não autorizado às informações contidas no mesmo.
- Os colaboradores, prestadores de serviços, fornecedores e/ou parceiros não poderão receber ou fornecer componentes dos equipamentos que utilizam, nem tampouco alterar sua localização, sem a prévia comunicação para a área administrativa.
- Não é recomendado comer ou beber próximo ao recurso de hardware ou em área onde possa ocorrer algum dano ao equipamento.
- Todos os equipamentos da instituição (inclusive notebooks quando houver) devem possuir algum tipo de proteção de tela, seja por senha ou qualquer outra forma de proteção, sendo esse para preservar o hardware de acessos indevidos.
- Todos os usuários dos notebooks autorizados são responsáveis pela guarda do mesmo e sempre devem estar ao seu alcance, não deixando em locais visíveis e/ou em áreas públicas (automóveis, taxis, shopping etc.). Quando estiver em viagens (terrestre, áreas, metroviárias etc.), deve ser transportado como bagagem de mão.

Normas de Uso de Dispositivos Externos

Não será permitido o uso de dispositivos externos nas estações de trabalho da rede como:

- Qualquer tipo de unidade de armazenamento de dados externo, como HD externo, unidades de USB etc., sem prévia autorização.

- Qualquer tipo de dispositivos de comunicação externa, como unidades de infraestrutura, dispositivo *Bluetooth*, sem prévia autorização.

- Qualquer tipo de leitura de dados externa e interna, como unidade de CD/DVD, USB etc. sem prévia autorização.

Placa fax modem ou modem não poderão ser instalados nem utilizados em estações de trabalho conectadas à rede, para conexão entre pontos remotos por meio de linha discada. Devem ser utilizadas somente conexões aprovadas (ex. *gateways, Proxy, firewalls*). Havendo necessidade incontornável de se estabelecer acesso remoto por meio da utilização desses recursos, deve-se buscar solução técnica apropriada.

Não é permitido o acesso remoto sem a devida autenticação do usuário (identificação do usuário e senha), estabelecendo o mecanismo de autenticação que será usado no acesso à rede.

Normas de Backup

- Visa proteger a instituição contra problema de disponibilidade e integridade. A cópia de segurança tem por finalidade permitir que as informações de um sistema ou arquivos em geral possam ser armazenadas de maneira off-line, criando um mecanismo que permite recuperá-la em caso de falha, modificação indevida ou exclusão.
- A XMS Investimentos utiliza o Google Drive, que faz o streaming dos arquivos do Drive diretamente da nuvem para os computadores físicos, liberando espaço em

disco e largura de banda da rede. Como os arquivos do Drive são armazenados na nuvem, as alterações feitas pelos seus colaboradores serão atualizadas automaticamente em todos os lugares.

- Também é possível disponibilizar arquivos do Drive para acesso off-line. Esses arquivos armazenados em cache serão sincronizados com a nuvem quando você estiver on-line, para que a versão mais recente esteja disponível em todos os seus dispositivos.
- O Google Drive possui a capacidade de guardar versões antigas dos arquivos. Sendo assim, caso um colaborador faça uma edição qualquer em um arquivo, o serviço automaticamente criará uma cópia que permitirá voltar ao estado anterior de seu trabalho, se assim for necessário.
- O Google Drive mantém até 100 revisões de um arquivo armazenadas em seu banco de dados, excluindo as mais antigas conforme novas edições forem detectadas, inclusive arquivos apagados.
- Além disso, é efetuado mensalmente uma cópia de todos os arquivos em outra conta de serviço de armazenamento em nuvem, no MS OneDrive.

Normas de Proteção Física

Esta norma procura proteger todas as informações no formato físico, guardando papéis que contém informações importantes, mídias etc. em locais protegidos e controlados. De forma geral destacamos as regras que devem ser seguidas:

- O acesso aos prédios e instalações da instituição deve ser controlado, sendo obrigatório o registro de entrada e o de saída de todos os colaboradores, prestadores de serviços, estagiários e visitantes.

- Todas as pessoas devem estar devidamente identificadas.

- Os equipamentos de infraestrutura de rede deverão estar em locais de acesso restrito e monitorado.

- Papéis e mídia magnética contendo informações confidenciais devem possuir controles de segurança adequados de armazenamento, impressão, manuseio e descarte.

- Todos os colaboradores devem manter as informações da instituição fora de alcance de pessoas não autorizadas, preservando seus locais de trabalho limpos e organizados, protegendo as informações em qualquer meio físico ou lógico, de acesso não autorizado.

- Todos os recursos de infraestrutura elétrica, prevenção de incêndios e de ar-condicionado que servem aos equipamentos de informática devem ser testados periodicamente, de acordo com as recomendações do fabricante.

- Circuito Fechado de TV pode ser usado para monitorar a eficiência de outros dispositivos de controles de acesso, além de gerar imagens que podem ser utilizadas após um incidente de segurança.

Dados Pessoais de Terceiros

As informações de terceiros são protegidas por lei na forma da Lei Geral de Proteção de Dados Pessoais (LGPD). Essa lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Os colaboradores da XMS Investimentos que efetuem o tratamento de dados pessoais devem cumprir a Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709, de 14 de agosto de 2018, podendo inclusive serem responsabilizados legalmente.

Os colaboradores da XMS Investimentos deverão assinar em campo específico do termo de adesão sobre o tratamento de dados pessoais de terceiros.

Responsabilidades

Os recursos e informações disponibilizados aos gestores de área, colaboradores, estagiários, fornecedores, demais colaboradores ou parceiros devem ser utilizados somente para os propósitos e finalidades aprovados pela instituição, de acordo com sua área de atuação.

Usuários

- Os usuários de sistema de informação são responsáveis pelo cumprimento das normas e procedimentos estabelecidos nesta política
- Utilização de sistemas de computação ou acesso de informações em qualquer meio somente quando autorizado pelos seus superiores e apenas para atividades aprovadas pela empresa
- Providenciar junto aos seus superiores o acesso aos recursos para exercer suas atividades diárias
- Utilização de todos os recursos tecnológicos existentes que sejam aprovados pela instituição para proteção de quaisquer tentativas de violação das informações, equipamentos, sistemas de computação ou outros recursos que contenham informações críticas aos negócios da sua Instituição.
- Execução de cópias de segurança na rede das informações que estiverem sob sua responsabilidade e/ou custódia
- Informação imediata ao seu superior, quando qualquer violação das políticas e procedimentos de segurança.

Gestores de área

Os gestores de área são responsáveis pelo (a):

- Informações que estão sob sua responsabilidade e de seus subordinados
- Garantia que os seus subordinados entendam e apliquem diariamente as políticas e os procedimentos referentes à segurança

- Autorização e revogação do acesso às informações e recursos necessários para que os colaboradores exerçam suas atividades
- Suporte aos seus subordinados quando das violações de segurança
- Participação da solução dos problemas relacionados a eventuais violações de segurança
- Estabelecimento de novos planos de ação para eliminar riscos e vulnerabilidades das informações
- Solicitação de redirecionamento das mensagens do funcionário ausente para outro usuário
- O compromisso de todos os gestores de área, colaboradores, prestadores de serviço, fornecedores e/ou parceiros no cumprimento das diretrizes estabelecidas é fundamental para a efetiva implementação desta política na empresa. O compromisso com a proteção previne que as informações sejam perdidas, falsificadas ou destruídas, acessadas por pessoas não autorizadas, roubadas ou alvo de espionagem.

Violação e Adesão

A violação ou não aderência aos procedimentos e normas constantes nesta **Política de Segurança da Informação e Cibernética** pelos colaboradores podem ocasionar ações disciplinares e, em alguns casos, até a demissão de um funcionário ou o cancelamento de um contrato de serviço. No caso de tratamento aos colaboradores, primeiramente será dada uma notificação verbal. Em caso de reincidência na infração, será dada uma notificação por escrito. Por fim, em caso de nova reincidência, o colaborador será desligado da empresa.

A adesão à **Política de Segurança da Informação e Cibernética** deve ser assinada em um **Termo de Adesão**, no qual o colaborador declara estar ciente das normas constantes na mesma. Esse termo detalhará todas as outras políticas da instituição, devendo ser assinado por todos os colaboradores da empresa. No caso de implementação ou modificação de qualquer política, bem como a instituição de novas políticas, novo termo deverá ser assinado pelos colaboradores da empresa, independente da prévia assinatura.

O responsável pela empresa em relação ao cumprimento da **Política de Segurança da Informação e Cibernética** e em relação aos órgãos regulares, clientes e demais agentes externos será um diretor previamente designado. Esse responderá por todos os questionamentos, adequações, auditorias, monitoramento e bom uso e cumprimento desta política pela empresa.

Os cumprimentos desses quesitos e as sanções cabíveis à empresa estão discriminados no **Manual de Controles Internos**. Essa dispõe sobre os mecanismos de cumprimento, monitoramento da conformidade das normas e demais políticas da empresa, além da adoção de medidas apropriadas em caso de infrações cometidas. Nessa política também constam os termos de adesão que devem ser assinados por gestores de área e demais colaboradores da organização.