POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

WNT CAPITAL DISTRIBUIDORA DE TÍTULOS E VALORES MOBILIÁRIOS S.A.

AGOSTO DE 2023

SUMÁRIO

Elaboração:	Ciência:	Aprovação:
Departamento de Segurança da Informação	Todos os Colaboradores da WNT Capital Distribuidora de Títulos e Valores S.A.	Diretoria Executiva

1. CONTROLE DE APROVAÇÃO

Versão	Data de Aprovação	Alterações	Classificação da Informação
1.0	07/03/2022	Versão Inicial	Pública
1.0	29.08.2023	Sem alterações	Pública

2. OBJETIVO

A presente Política de Segurança da Informação ("Política") da WNT Capital Distribuidora de Títulos e Valores Mobiliários S.A. ("WNT DTVM" ou "Instituição") visa promover a confidencialidade, integridade e disponibilidade no manuseio e tratamento de informações em suas mais variadas formas.

Toda informação relacionada às operações da WNT DTVM, gerada ou desenvolvida nas dependências desta, durante a execução das atividades dos Colaboradores e de Prestadores de serviços, constitui ativo desta instituição, essencial à condução de negócios, e em última análise, à sua existência.

Independentemente da forma apresentada ou do meio pelo qual é compartilhada ou armazenada, a informação deve ser utilizada unicamente para a finalidade para a qual foi autorizada.

3. ABRANGÊNCIA

Todos os colaboradores e terceirizados que prestem serviços direta ou indiretamente relacionados à WNT DTVM estão sujeitos às diretrizes descritas na presente Política.

4. RESPONSABILIDADES

É missão e responsabilidade de cada Colaborador, estagiário, prestador de serviço, parceiro ou visitante à WNT DTVM, observar e seguir as políticas, padrões, procedimentos e orientações estabelecidas para o cumprimento da presente Política, além de toda legislação vigente.

É imprescindível que cada pessoa compreenda o papel da segurança da informação em suas atividades diárias.

Quanto ao Departamento de Segurança da Informação, é de sua responsabilidade específica:

i. Controlar e monitorar qualquer tipo de acesso à internet fornecido pela WNT DTVM;
ii. Reportar eventuais tentativas de acesso não autorizados ou incidentes de segurança relacionados ao acesso internet para a Diretoria Executiva.
iii. Avaliar, aprovar ou negar solicitações para uso de acesso remoto a ativos/serviços de informação ou recursos computacionais da WNT DTVM;
iv. Controlar e monitorar qualquer tipo de acesso remoto fornecido pela WNT DTVM;
v. Tratar eventuais tentativas de acesso não autorizados ou incidentes de segurança relacionados ao acesso remoto e, quando pertinente, reportar estes para a Diretoria Executiva;
vi. Definir a classificação das informações junto com um Gestor definido por ele, do departamento, com base nas categorias de classificação constantes desta norma, mantendo um registro atualizado dos itens classificados;

vii. Esse Gestor deverá controlar as informações geradas em seu departamento de negócio e atuação;

viii. Revisar periodicamente a classificação das informações sob sua guarda;

ix. Realizar o monitoramento dos ativos/serviços de informação ou recursos computacionais da WNT DTVM;

x. Tratar eventuais violações das diretrizes de segurança da WNT DTVM identificadas através de ferramentas de monitoramento, e, quando pertinente, reportar estas ao departamento de segurança da informação;

xi. Tratar casos de infecção ou suspeita de infecção por códigos maliciosos, reportando estes ao departamento de segurança da informação, caso necessário;

xii. Garantir que novas modalidades de códigos maliciosos são adequadamente investigadas, tratadas e protegidas, pela ferramenta corporativa adotada pela WNT DTVM;

xiii. Garantir a existência de iniciativas para divulgação sobre informações de ameaças, códigos maliciosos e medidas de proteção para os usuários da WNT DTVM;

xiv. Atuar como responsável por ocorrências e eventos de segurança e garantir a existência de recursos identificar, escalar, mitigar, conter, e erradicar incidentes de segurança, bem como ações efetivas para recuperar o estado anterior de ativos/serviços de informação ou recursos computacionais afetados pelo incidente;

xv. Comunicar prontamente o departamento de resposta a incidentes de segurança da informação da WNT DTVM sobre eventos e incidentes de segurança;

xvi. Estabelecer e manter atualizados os procedimentos complementares a esta norma;

xvii. Comunicar ao responsável pelo Departamento de Segurança da Informação eventuais tentativas, bem-sucedidas ou não, de desvio de conduta dos termos dessa norma;

xviii. Avaliar, aprovar ou negar solicitações para uso de dispositivos pessoais no ambiente corporativo.

xix. Controlar e monitorar os serviços de e-mail e comunicadores instantâneos fornecidos pela Instituição;

xx. Reportar eventuais tentativas de violação dos termos desta norma ou incidentes de segurança relacionados ao uso dos serviços de e-mail e comunicadores instantâneos para o departamento de segurança da informação.

xxi. Avaliar, aprovar ou negar solicitações para uso de acesso remoto a ativos/serviços de informação ou recursos computacionais da WNT DTVM.

xxii. Controlar e monitorar qualquer tipo de acesso remoto fornecido pela WNT DTVM;

xxiii. Tratar eventuais tentativas de acesso não autorizados ou incidentes de segurança relacionados ao acesso remoto e, quando pertinente, reportar estes ao responsável pelo Departamento de Segurança da Informação.

5. CONFIDENCIALIDADE

São consideradas informações confidenciais, para os fins desta Política:

a) *Qualquer informação, escrita ou verbal, apresentada de modo tangível ou intangível, podendo incluir know-how, técnicas, cópias, diagramas, modelos, amostras, programas de computador, informações técnicas, financeiras ou relacionadas a estratégias comerciais, incluindo saldos, extratos e posições de clientes e dos fundos administrados e/ou geridos pela* WNT DTVM*, operações estruturadas, demais operações e seus respectivos valores, estruturas, planos de ação, relação de clientes, contrapartes comerciais, fornecedores e prestadores de serviços, bem como informações estratégicas, mercadológicas ou de qualquer natureza pertinentes às atividades da* WNT DTVM*; e*

b) *Informações acessadas pelo Colaborador em função do desempenho de suas atividades na WNT DTVM, bem como informações estratégicas ou mercadológicas de qualquer natureza, obtidas junto aos sócios, administradores, ou funcionários da Sociedade, ou, ainda, junto aos seus representantes, consultores, assessores, clientes, fornecedores e prestadores de serviços em geral.*

Aquele que receber as informações confidenciais deverá mantê-las e resguardá-las em caráter sigiloso, bem como limitar seu acesso, controlar quaisquer cópias de documentos, dados e reproduções que porventura sejam extraídas desta.

As cláusulas de ciência, responsabilidade e confidencialidade quanto à política e diretrizes de segurança da informação visam alertar e responsabilizar todos, de que o acesso e o manuseio de informação devem se restringir ao exercício da função ou processo que requer essa informação, sendo proibido o uso para qualquer outro propósito distinto do designado.

6. NORMAS DE SEGURANÇA DA INFORMAÇÃO

A presente Política estabelece normas de segurança de informação para específicas atividades, de modo que o grau de monitoramento e sistemas de segurança sejam condizentes com o risco de atividade atrelada à WNT DTVM.

6.1. Normas de acesso à internet e comportamento em mídias sociais

Esta Norma estabelece diretrizes para utilização segura do acesso à internet fornecido pela WNT DTVM e do comportamento de colaboradores em mídias e redes sociais.

A WNT DTVM fornece acesso à Internet aos seus usuários autorizados, conforme as necessidades inerentes ao desempenho de suas atividades profissionais, sendo que o acesso à internet pode ser fornecido tanto através da rede corporativa, quanto através da disponibilização de serviços de internet móvel

Toda informação que é acessada, transmitida, recebida ou produzida através do acesso à internet está sujeita monitoramento, não havendo por parte do usuário qualquer expectativa de privacidade;

Durante o acesso à Internet fornecido pela WNT DTVM não será permitido o download, o upload, a inclusão, a disponibilização, a visualização, a edição, a instalação, o

armazenamento e/ou a cópia de qualquer conteúdo relacionado expressa ou subjetivamente, direta ou indiretamente, com atividades ilícitas ou contrárias à legislação vigente.

A publicação de conteúdo referente à WNT DTVM em mídias e redes sociais é feita por setores e usuários que possuem essa responsabilidade específica, sendo os demais usuários proibidos de publicar qualquer tipo de informação em nome da instituição;

6.2. Normas de acesso remoto

Esta norma estabelece normas e diretrizes para o acesso remoto a ativos/serviços de informação e recursos computacionais da WNT DTVM, garantindo níveis adequados de proteção a estes.

Em casos de acesso não autorizado, extravio, furto ou roubo de dispositivos computacionais que possuam o acesso remoto ao ambiente da WNT DTVM habilitado, o usuário responsável deverá informar imediatamente o ocorrido departamento de segurança da informação.

Durante o monitoramento do acesso remoto a seus ativos/serviços de informação ou recursos computacionais, a WNT DTVM se resguarda o direito de, sem qualquer notificação ou aviso, interceptar, registrar, gravar, ler, copiar e divulgar por, ou para, pessoas autorizadas para finalidades oficiais, incluindo investigações criminais, toda informação trafegada, seja originada de sua rede interna e destinada a redes externas ou o contrário.

6.3. Norma de classificação e manuseio da informação

Esta Norma estabelece diretrizes para a classificação, manuseio e rotulagem dos ativos de informação da WNT DTVM por seus usuários autorizados.

6.4. Classificação e rotulagem da Informação:

Para efeitos de classificação da informação, a WNT DTVM utiliza as seguintes categorias:

INFORMAÇÃO PÚBLICA: Informação oficialmente liberada pela WNT DTVM para o público geral. A divulgação deste tipo de informação não causa problemas a WNT DTVM ou a seus clientes, podendo ser compartilhada livremente com o público geral, desde que seja mantida sua integridade.

INFORMAÇÃO INTERNA: Informação que pode ser compartilhada internamente com todos os colaboradores da WNT DTVM, no entanto, não podendo ser compartilhada para o público geral.

INFORMAÇÃO RESTRITA: Informação liberada exclusivamente para usuários e departamentos específicos da WNT DTVM, não podendo ser compartilhada com o público em geral. Estas informações só podem ser compartilhadas mediante autorização expressa.

INFORMAÇÃO CONFIDENCIAL: Informação de caráter sigiloso, podendo ser comunicada exclusivamente a usuários especificamente autorizados e que necessitem conhecê-las para o desempenho de suas tarefas profissionais na WNT DTVM A divulgação ou alteração não autorizada desse tipo de informação pode causar graves danos e prejuízos para a WNT DTVM e/ou seus clientes, portanto seu compartilhamento deve ser restrito e feito de maneira controlada.

A classificação da informação deverá ser realizada pelos gestores da informação, considerando este o responsável pela elaboração do documento, ou colaboradores designados por estes. Entretanto, a responsabilidade pela assertividade do nível selecionado permanece com o gestor da informação;

O descarte da informação deve ser realizado de forma a impedir a recuperação desta, independente do seu formato de armazenamento original;

6.5. Normas de gestão de identidade e controle de acesso

Esta Norma estabelece diretrizes para gestão de identidade e acesso aos ativos e sistema de informação da WNT DTVM.

A WNT DTVM fornece a seus usuários autorizados contas de acesso que permitem o uso de ativos de informação, sistemas de informação e recursos computacionais como, por exemplo, rede corporativa;

As referidas contas de acesso são fornecidas exclusivamente para que os usuários possam executar suas atividades laborais;

Toda conta de acesso, assim como suas senhas pessoais do usuário são de uso pessoa e intransferível. Desta forma, o usuário é integralmente responsável por sua utilização, respondendo por qualquer violação ou ato irregular/ilícito, mesmo que exercido por outro indivíduo e/ou instituição de posse de sua conta de acesso.

Os usuários deverão adotar medidas de prevenção para garantir o acesso seguro a ativos e serviços de informação.

A autorização e o nível permitido de acesso ativos/serviços de informação da WNT DTVM é feita com base em perfis que definem o nível de privilégio dos usuários.

Autorizações de acesso a perfis são fornecidas e/ou revogadas com base na solicitação dos gestores de cada colaborador. Solicitações deverão ser encaminhadas ao departamento de tecnologia da informação.

6.6. Norma de proteção contra códigos maliciosos

Esta norma tem como objetivo, estabelecer diretrizes para a proteção dos ativos/serviços de informação da WNT DTVM contra ameaças e códigos maliciosos de qualquer natureza.

A WNT DTVM disponibiliza ferramentas para proteção dos seus ativos/serviços de informação e recursos computacionais, incluindo estações de usuários, dispositivos móveis e servidores corporativos, contra ameaças e códigos maliciosos tais como vírus, cavalos de Tróia, vermes, ferramentas de captura de tela e dados digitados, softwares de propaganda e similares;

Apenas a ferramenta disponibilizada pela WNT DTVM deve ser utilizada na proteção contra códigos maliciosos;

A ferramenta de proteção contra códigos maliciosos da WNT DTVM adota as seguintes regras de uso:

Atualização em tempo real do arquivo de assinaturas de códigos maliciosos e varredura diária em estações de usuários e servidores corporativos;

As varreduras diárias devem analisar todos os arquivos em cada uma das unidades de armazenamento locais das estações de usuários e dispositivos móveis;

As varreduras diárias em servidores corporativos podem ser limitadas a pastas ou arquivos específicos, de modo a evitar o comprometimento do desempenho de recursos computacionais críticos;

As funções de proteção em tempo real e detecção com base no comportamento devem estar habilitadas para todas as estações de usuários e dispositivos móveis;

Sites, serviços e arquivos baixados da internet detectados como possíveis ameaças serão automaticamente bloqueados em estações de usuários, dispositivos móveis e servidores corporativos;

Mesmo com a existência de ferramentas para proteção contra códigos maliciosos, os usuários da WNT DTVM devem adotar um comportamento seguro, reduzindo a probabilidade de infecção ou propagação de códigos maliciosos;

Os usuários devem seguir as seguintes regras para proteção contra códigos maliciosos:

Não tentar efetuar o tratamento e correção de códigos maliciosos por iniciativa própria;

Reportar imediatamente o departamento de tecnologias da informação qualquer infecção ou suspeita de infecção por código malicioso;

Não desenvolver, testar ou armazenar qualquer parte de um código malicioso de qualquer tipo, a menos que expressamente autorizado;

Efetuar uma varredura com a ferramenta de proteção contra códigos maliciosos fornecida pela WNT DTVM antes de utilizar arquivos armazenados em mídias removíveis, baixados da internet ou recebidos nos serviços de e-mail ou comunicadores instantâneos;

Não habilitar MACROS para arquivos recebidos de fontes suspeitas, baixados da internet ou recebidos nos serviços de e-mail ou comunicadores instantâneos. Caso necessário, poderá ser solicitado o apoio do departamento de segurança da informação para validar se o arquivo representa ou não uma ameaça.

6.7. Norma de resposta a incidente de segurança da informação

Esta norma estabelece diretrizes para garantir a resposta e tratamento adequados a incidentes de segurança da informação que possam impactar ativos/serviços de informação ou recursos computacionais do WNT DTVM.

6.8. Norma de armazenamento de informação

A WNT DTVM disponibiliza para seus usuários espaço para armazenamento remoto de arquivos na nuvem, através de sua solução corporativa, garantindo nível máximo de segurança.

Não é permitido o uso de qualquer outra solução de armazenamento na nuvem, que não seja a oficialmente adotada pela empresa e homologada pelo departamento de segurança da informação da WNT DTVM.

As instalações de processamento das informações da WNT DTVM serão mantidas em áreas seguras, cujo perímetro é fisicamente isolado contra o acesso não autorizado, os danos e quaisquer interferências de origem humana ou natural.

6.9. Norma de uso de serviços de e-mail e comunicadores instantâneos

Esta norma estabelece diretrizes para utilização segura dos serviços de e-mail e comunicadores instantâneos fornecidos por WNT DTVM.

6.9.1. Serviço de e-mail

A WNT DTVM fornece o serviço de e-mail para seus usuários autorizados exclusivamente para o desempenho de suas atividades profissionais;

Não é permitido o uso de qualquer serviço de e-mail, que não seja o oficialmente fornecido pela WNT DTVM;

O monitoramento do serviço de e-mail da WNT DTVM tem como objetivos proteger a instituição, atestar o respeito às regras contidas nessa norma, bem como produzir evidências relativas à eventual violação destas e/ou à legislação em vigor;

6.9.2. Serviços de Comunicadores instantâneos

A WNT DTVM, fornece o serviço de comunicadores instantâneos para seus usuários autorizados, exclusivamente para o desempenho de suas atividades profissionais;

Não é permitido o uso de qualquer serviço de comunicadores instantâneos, que não seja o oficialmente homologado pela WNT DTVM;

O monitoramento do serviço de comunicadores da WNT DTVM tem como objetivos proteger a instituição, atestar o respeito às regras contidas nessa norma, bem como produzir evidências relativas à eventual violação destas e/ou à legislação em vigor;

7. PENALIDADES

As violações de segurança devem ser informadas ao departamento de Segurança da Informação, de modo que toda violação ou desvio é investigado para a determinação das medidas necessárias, visando à correção da falha ou reestruturação de processos.

A WNT DTVM estabelece penalidades para aqueles que deixem de cumprir os procedimentos estabelecidos em suas políticas, manuais, procedimentos e demais regras internas, abrangendo as esferas cível, criminal, trabalhista e administrativa.

As principais penas as quais os Colaboradores da WNT DTVM estão sujeitos são:

- Advertência;
- Multas (em espécie ou em perda direta de benefícios ou de possíveis pontos de avaliação para fins de remuneração variável);
- Suspensão; e
- Demissão por justa causa.

Todos os Colaboradores estarão sujeitos às ações judiciais de natureza criminal, cível e administrativa, bem como às sanções internas disciplinares, incluindo seu possível desligamento em caso de descumprimento de qualquer legislação, regulamentação ou de qualquer procedimento relativo à presente Política.

8. ATUALIZAÇÕES

Em atenção às legislações aplicáveis, bem como às diretrizes aqui prevista, esta Política será revisada em prazo não superior a 12 (doze meses), devendo ser observadas eventuais necessidades de atualização em momento antecedente.

****