Wealth High Governance

Dezembro de 2023 – Versão 5.0

Política de Segurança da Informação e Segurança Cibernética

Índice

1. Introdução e Objetivos

Todo e qualquer usuário de recursos computadorizados da nossa instituição tem a responsabilidade de proteger a segurança e a integridade das informações e dos equipamentos de informática.

Em linha com as principais discussões e preocupações do mercado, a Política tem como base princípios e procedimentos que asseguram a confidencialidade, a disponibilidade e a integridade dos dados e sistemas de informação.

Esta Política tem por objetivo contribuir para o aprimoramento da segurança, tanto informacional quanto cibernética da WHG, estabelecendo medidas a serem tomadas para identificar e prevenir ações que possam causar prejuízo para a WHG e seus clientes.

Em atenção aos dispositivos da Instrução CVM n.º 21/21, do Código ANBIMA de Regulação e Melhores Práticas para Administração e Gestão de Recursos de Terceiros e da Resolução BACEN nº 4.893/21, a WHG procurou identificar os eventos com maior possibilidade de ocorrência, bem como as informações mais sensíveis (“Informações Confidenciais”), com o propósito de mitigar os riscos à sua atividade e seus clientes.

As Informações Confidenciais devem seguir o princípio *need-to-know* / *need-to-have*. Sendo assim, nenhuma informação confidencial deve, em qualquer hipótese, ser divulgada a pessoas, dentro ou fora da WHG, que não necessitem ou não devam ter acesso a elas para desempenho de suas atividades.

Qualquer informação sobre a WHG, ou de qualquer natureza relativa às atividades da empresa e a seus sócios e clientes, obtida em decorrência do desempenho das atividades normais dos Colaboradores, só poderá ser fornecida ao público, mídia ou a demais órgãos caso autorizado pelo Diretor de Risco e *Compliance*.

A Diretoria Executiva está comprometida com a melhoria contínua dos procedimentos relacionados à segurança cibernética.

2. Abrangência

A Política se aplica a todos os colaboradores da Wealth High Governance Asset Management Ltda., da Wealth High Governance Capital Ltda. e da Wealth High Governance DTVM S.A. (em conjunto denominadas “WHG”), incluindo trabalhos executados externamente ou por terceiros que utilizem o ambiente da WHG, ou que acessem informações a ela pertencentes.

3. Diretrizes

3.1 Segurança da Informação

A Segurança da Informação na WHG é estabelecida com base nas seguintes diretrizes:

I. As informações da WHG, dos clientes e do público em geral devem ser tratadas de forma ética e sigilosa e de acordo com as leis vigentes e normas internas, evitando-se mau uso e exposição indevida.

II. As informações devem ser utilizadas de forma transparente e apenas para a finalidade para a qual foram coletadas.

III. Todo processo e ação que acontece no âmbito da WHG deve seguir as normas e regras de segregação de funções.

IV. O acesso às informações e recursos deve ser feito mediante autorização, de forma identificável, única e intransferível.

V. A concessão de acessos deve obedecer ao critério de menor privilégio, no qual os usuários têm acesso somente aos recursos de informação imprescindíveis para o desempenho de suas atividades.

VI. A senha é utilizada como assinatura eletrônica e deve ser mantida secreta, sendo proibido seu compartilhamento.

VII. Todo Colaborador deve reportar, assim que identificados, os riscos às informações diretamente para a área de TI da WHG.

VIII. A área de TI deve divulgar amplamente as regras e responsabilidades relacionadas à Segurança da Informação para os Colaboradores, e estes devem entender e assegurar seu cumprimento.

3.2 Segurança Cibernética

Com o aumento exponencial de ameaças cibernéticas, através de métodos como implantação de *malware*, uso de engenharia social, ataques de DDoS *(distributed denial of services) e botnets* ou invasões**,** potencializado pelo avanço tecnológico e a ampliação dos meios de comunicação, a WHG instituiu em sua estrutura, adequados procedimentos para a identificação e mitigação dos riscos, assim como para se recuperar de eventuais incidentes.

Com isso a WHG visa estabelecer procedimentos para cada uma das seguintes etapas: (i) identificação dos riscos e atividades essenciais à WHG; (ii) implementação de ações de proteção e prevenção; (iii) implementação de controles, monitoramento e testes; e (iv) criação de um plano de respostas além da manutenção constante deste mecanismo.

Todas as diretrizes aqui dispostas são de responsabilidade da área de Tecnologia da Informação (“TI”) da WHG.

4. Programa de Segurança da Informação e Cibernética

4.1 Estrutura de TI

Segue lista com os principais equipamentos, procedimentos e sistemas de TI da WHG:

- *Backup* diário
- Servidores
- *Switches*
- *Laptops*
- *Desktops*
- *Firewall*
- *Links* dedicados de provedores distintos
- Conexão com a Internet
- Telefonia e PABX
- EDR
- Sistema de informações de posição dos fundos
- Sistemas de prevenção ao vazamento de dados
- Sistema de correio eletrônico com *anti-spam* e recursos de regras para controle de envio de e-mails
- Nobreak com gerenciamento, para prevenção de surtos elétricos e estabilização elétrica de todas as tomadas dos equipamentos sensíveis da empresa, como os ativos de TI e mesa de operação
- CPD em local climatizado com sistema de ar-condicionado redundante e com monitoramento de temperatura e com acesso restrito ao local

Ainda os seguintes procedimentos são efetuados pelo time de TI: análise e correção de vulnerabilidades, contratação e implementação de *Pentest* (teste de intrusão) para validação de possíveis falhas em código, duplo fator de autenticação nos acessos, segregação de acessos por função e área, criptografia dos dados.

4.2 Propriedade dos Recursos de TI

Todos os recursos computacionais e de sistemas disponibilizados para os Colaboradores são de propriedade da WHG.

Em relação aos sistemas disponibilizados por terceiros e contratados pela WHG, o devido suporte técnico aos usuários está previsto nos respectivos acordos comerciais.

4.3 Classificação da Informação

Para o compartilhamento de informações, devem sempre ser consideradas as necessidades relacionadas ao negócio, o compartilhamento ou restrição de acesso e os impactos no caso de utilização indevida das informações.

As informações são rotuladas nos seguintes níveis:

Informação Confidencial – Classificação para dados sigilosos considerados sensíveis, a qual o acesso é restrito pela lei ou regulamentos, devendo ser distribuídos apenas para pessoas autorizadas.

Informação Interna – Classificação para dados institucionais, ou seja, que apenas devem ser distribuídos internamente.

Informação Pública – Classificação para dados de divulgação ilimitada, indicando acesso e uso irrestrito.

Informação Restrita – Classificação para dados que precisam de proteção de acesso não autorizado, inclusive internamente para segregação de funções e atividades, visando evitar conflitos de interesse ou danos ao negócio.

Tais definições foram previamente estabelecidas de acordo com a confidencialidade e as proteções mínimas necessárias e devem receber os tratamentos cabíveis, conforme conceitos nesta Política.

4.4 Controles de Acesso

Todos os computadores disponibilizados para os Colaboradores da WHG têm por objetivo o desempenho das suas atividades profissionais e não devem ser utilizados para quaisquer outros fins.

Todos os acessos aos sistemas são liberados com base no conceito de *need-to-know / need-to-have* e todo o processo de criação e exclusão de usuário, instalação de *softwares* e aplicativos, permissão de acesso, entre outras funcionalidades

informáticas, são realizados pela área de TI, com base em perfis ou grupos de acesso do *Active Directory*.

A disponibilização e uso dos computadores da WHG respeitam as seguintes regras:

- Todos os equipamentos, *software*s e permissões de acessos devem ser testados e autorizados pela área responsável pelas informações;
- Cada computador tem o seu usuário gestor, que é responsável por esse equipamento;
- Os parâmetros de senhas utilizados na WHG são veiculados apenas internamente para os colaboradores.

4.5 *Softwares*

A implantação e configuração de *software*s da WHG respeitam as seguintes regras:

- Todos os *software*s, programas básicos (sistema operacional e ferramentas) e componentes físicos são implantados e configurados pela área de TI;
- É vedado ao usuário implantar ou alterar componentes físicos em seus computadores;
- Somente é permitido o uso de equipamentos homologados e devidamente contratados pela WHG;
- A utilização de equipamentos pessoais por terceiros nas instalações da WHG e a conexão destes na rede interna à Internet requer autorização prévia;
- Os Colaboradores estão autorizados a conectar seus telefones celulares e computadores pessoais diretamente à internet;
- A conexão de dispositivos móveis de armazenamento (e.g. USB *Drive*) somente poderá ser realizada mediante autorização prévia.

4.6 Registros

A WHG mantém por 5 (cinco) anos todos os *logs* de sistemas, e verifica regularmente, quaisquer desvios de padrão em todos os computadores, arquivos em rede, *software*s, *hardwares* ou acessos que não foram autorizados.

Nesse sentido, através dos *logs* realizados, a WHG consegue manter a integridade, autenticidade assim como o rastreamento dos acessos e das informações e sistemas.

4.7 Responsabilidades do Usuário

Os Colaboradores são os custodiantes e responsáveis pelos recursos disponibilizados a eles, devendo estes cuidarem adequadamente deles.

Os Colaboradores devem garantir a integridade física e o perfeito funcionamento dos recursos, seguindo as regras e orientações fornecidas pela WHG.

Ainda, os Colaboradores devem adotar um comportamento seguro, condizente com esta Política, e devem seguir, minimamente, as seguintes diretrizes:

- Não compartilhar nem divulgar senha a terceiros;
- Não discutir assuntos confidenciais relacionados a suas atividades em ambientes públicos ou em áreas expostas (aviões, restaurantes, encontros sociais etc.);
- Não abrir mensagens de origem desconhecida, ou clicar em *links* que sejam suspeitos, mesmo que advindos de origem conhecida;
- Armazenar e proteger adequadamente documentos impressos e arquivos eletrônicos que contêm Informações Confidenciais; e
- Seguir corretamente as regras estabelecidas nessa política para uso de internet e correio eletrônico.

4.8 Regras e Responsabilidades do Uso da Internet

Os Colaboradores são responsáveis por todo acesso realizado com a sua autenticação. Quando o usuário se comunicar através de recursos de TI da WHG, este deve sempre resguardar a imagem da WHG, evitando entrar em sites de fontes não seguras, assim como de abrir e-mails suspeitos.

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;
- 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;

- Possuam origem suspeita ou que não se atenham aos padrões de segurança adequados, assim como possuam *links* suspeitos.

O usuário deve garantir que está cumprindo a legislação em relação ao direito autoral, licença de uso e patentes existentes e que o uso de qualquer material foi devidamente autorizado.

4.9 Bloqueio de Endereços de Internet

Periodicamente, a área de TI irá revisar e bloquear o acesso para os endereços da Internet que não estejam alinhados com esta Política e com o Código de Ética da WHG.

4.10 Uso de Correio Eletrônico

O endereço eletrônico disponibilizado para o usuário é individual, intransferível e pertence à WHG.

O endereço eletrônico cedido para o usuário deve ser o mesmo durante todo o seu período de vínculo com a WHG, no entanto, se houver necessidade de troca de endereço, a alteração será realizada pela área de TI.

4.11 Endereço Eletrônico de Programas ou de Comunicação Corporativa

É permitido que um programa aplicativo ou um programa de sistema possua um endereço de correio eletrônico.

É permitida a existência de endereços de correio eletrônico para o envio de mensagens tipo Comunicação Interna da WHG.

O endereço de correio eletrônico disponibilizado para os Colaboradores e as mensagens associadas a este correio eletrônico são de propriedade da WHG.

4.12 Acesso à Distância ao E-mail

O usuário pode acessar o correio eletrônico cedido pela WHG mesmo quando estiver fora do ambiente da empresa, através do *app Outlook* em aparelhos de celular ou do serviço de VPN, tecnologia que cria uma conexão criptografada, promovendo uma comunicação segura na transmissão de dados.

O Colaborador deve ter o mesmo zelo com a utilização do correio eletrônico à distância tal qual estivesse no ambiente físico da WHG.

4.13 Responsabilidades e Forma de uso de Correio Eletrônico

O Colaborador que utiliza um endereço de correio eletrônico é responsável por todo acesso, conteúdo de mensagens e uso relativos ao seu e-mail, podendo enviar mensagens necessárias para o seu desempenho profissional na WHG.

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;
- 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 suscetíveis 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 WHG;
- Sejam incoerentes com o Código de Ética da WHG.
- É proibido reproduzir qualquer material recebido pelo correio eletrônico ou outro meio, que possa infringir direitos de autor, marca, licença de uso de programas ou patentes existentes, sem que haja autorização expressa do autor do trabalho e da organização.

Os Colaboradores devem estar cientes que uma mensagem de correio eletrônico da WHG é um documento formal e, portanto, possui as mesmas responsabilidades de um documento convencional da entidade.

Exceto quando especificamente autorizado para tal, é proibido emitir opinião pessoal, colocando-a em nome da WHG.

Deve observar se o endereço do destinatário corresponde realmente ao destinatário desejado.

Os Colaboradores devem ser diligentes no mínimo em relação:

- Aos usuários que receberão a mensagem (Destinatário/ To, Copiado/Cc e Copiado Oculto/Bcc);
- Ao nível de sigilo da informação contida na mensagem;
- Aos anexos da mensagem, enviando os arquivos apenas quando for imprescindível e garantindo a confidencialidade;
- Ao uso da opção encaminhar (*Forward*), verificando se é necessária a manutenção das diversas mensagens anteriores que estão encadeadas.

4.14 Cópias de Segurança do Correio Eletrônico

Para que seja possível uma gestão segura, efetiva, confiável, administrável e passível de auditoria a cópia de segurança das mensagens de correio eletrônico é feita de forma centralizada.

4.15 Armazenamento em Nuvem (*Cloud*)

A WHG realiza o armazenamento das Informações Confidenciais e quaisquer outros dados na Nuvem (*Cloud*).

Para tal armazenamento a WHG possui um ambiente seguro de nuvem, considerando aplicações WEB, e que preza pela confiabilidade, disponibilidade e integridade de armazenamento. A contratação dos serviços de processamento e armazenamento de dados em nuvem deve seguir os procedimentos exigidos pela Resolução BACEN nº 4.893/21.

4.16 Segurança Física dos Ambientes de Operação e Processamento

Para a segurança dos ambientes de operação e processamento da WHG, são estabelecidas diretrizes que visam garantir a proteção da infraestrutura tecnológica contra o acesso físico não autorizado, danos e interferências nas instalações e informações, assim como a perdas, danos, furto ou comprometimento de ativos e interrupção das atividades operacionais, através de controles, gestão e resposta aos incidentes.

Os equipamentos e instalações de processamento são mantidos em áreas seguras, garantidas por níveis de controle de acesso adequados, bem como proteção contra ameaças físicas e ambientais, observados os seguintes procedimentos:

- Utilização de credencial de acesso individualizados e passíveis de bloqueio e restrições;
- Exclusão de autorizações concedidas a Colaboradores afastados ou desligados e alteração no caso de mudança de atividade dentro da WHG;
- Revisão periódica das autorizações de acesso;
- Sistema de segurança por videomonitoramento das instalações físicas;
- Proteção contra ameaças externas por meio da segregação das áreas de entrega e carregamento.

Para a segurança dos recursos, a WHG adota medidas para garantir que os recursos redundantes não estejam sujeitos aos mesmos riscos físicos e ambientais que os recursos principais, inclusive contra falta de energia elétrica e outras interrupções provocadas por falhas das utilidades, segurança do cabeamento, manutenção de equipamentos, reutilização e alienação segura de equipamentos, e, por fim, remoção de propriedade.

5. Monitoramento e Testes Periódicos

O monitoramento dos controles existentes e estabelecidos nessa Política serão realizados e executados pela área de TI. Este acontecerá de forma contínua, sem periodicidade preestabelecida. Para tanto, a WHG dispõe de tecnologias de defesa baseadas em antivírus com *firewall de end-point*; criptografia dos discos dos Colaboradores; *firewall* físico com redundância para o escritório; VPN com duplo fator de autenticação; além de duplo fator de autenticação para as contas dos usuários.

Os Testes de Contingência serão realizados periodicamente, de modo a permitir que a WHG esteja preparada para a continuidade de suas atividades, assim como a mitigar eventuais riscos operacionais ou reputacionais. Outras informações sobre dos Testes de Contingência estão no Plano de Continuidade de Negócios da WHG.

Ademais, serão realizados Testes Periódicos de Segurança, com especial enfoque em segregação lógica, resposta a eventos de vazamento de dados, rastreabilidade dos *logs* de acessos às informações sensíveis, tratamento de dados, dentre outros, sempre objetivando a preservação dos dados mantidos pela WHG, em especial os confidenciais.

Ainda, serão realizados testes periódicos contendo a simulação de comunicações com *links* maliciosos, prática em que os *hackers* utilizam os dados coletados da engenharia social para ter credibilidade e enganar vítimas, podendo comprometer estações de trabalho, "*Phishing*", visando confirmar se os colaboradores estão conscientes dessas possíveis tentativas de fraudes.

Referidos testes serão realizados periodicamente e o resultado é consolidado no relatório anual de controles internos da WHG.

Periodicamente a área de TI, e a área de *Compliance*, realizam reuniões de governança com o intuito de compartilhar informações sobre novas tecnologias, produtos, ameaças, vulnerabilidades, gerenciamento de risco, políticas de segurança e outras atividades relativas à segurança corporativa, de modo a prover o conhecimento das práticas mais modernas e adequadas para a proteção de suas informações. Nessa reunião a área de segurança elabora um relatório consolidado das ameaças e vulnerabilidades tratadas pelo monitoramento contínuo, e as classificações de cada tratativa.

6. Tratamento de Incidentes

Os incidentes de segurança da informação, tais como indícios, suspeitas fundamentadas, vazamento de Informações Confidenciais ou qualquer outro incidente que caracterize falha de segurança devem ser reportados imediatamente através do e-mail whg.infra@whg.com.br que são direcionados para atuação da área de TI.

Na atuação de reporte acima, inclusive em decorrência da ação de criminosos cibernéticos, as providências pertinentes deverão ser iniciadas, devendo cada área responsável agir conforme o disposto na presente Política. A depender do caso, a WHG pode contratar empresa de tecnologia da informação terceirizada para tratamento e combate ao incidente, bem como nas respostas ao eventual dano.

Estas providências consistem, dentre outras, em:

I. Verificação e auditoria dos *logs*;

II. Criação de laudo pericial contendo as informações que foram potencialmente vazadas;

III. Execução de aplicativos externamente ou em sistemas afetados para eliminar aplicativos indesejados;

IV. Desinstalação de *software*;

V. Desativação de contas comprometidas e aplicação de políticas de restrição de acesso;

VI. Isolamento de sistemas afetados para evitar movimentação lateral e a propagação do incidente;

VII. Execução de varreduras *offline* para descobrir quaisquer ameaças adicionais;

VIII. Formatação e reconstrução do sistema operacional;

IX. Substituição física de dispositivos de armazenamento

X. Reconstrução de sistemas e redes;

XI. Restauração de dados provenientes do *backup*;

XII. Remoção de *malware* e artefatos relacionados;

XIII. Correção de vulnerabilidades identificadas que permitiram o incidente.

Todo e qualquer incidente ocorrido contará com a abertura de chamado de incidentes de segurança e classificação por nível de severidade, sendo que tais dados, assim como os resultados do plano de resposta, deverão ser arquivados e documentados, bem como ser formalizados no Relatório de Controles Internos da WHG.

6.1. Classificação de Incidentes de Segurança da Informação

Verificada a ocorrência de incidentes de segurança, a WHG atribuirá o nível de criticidade do incidente de acordo com parâmetros definidos internamente, conforme segue:

- **Muito alto (Impacto Grave)** – Incidente com potencial de interromper todas as operações e processos críticos por um longo período. Evento que pressupõe um dano financeiro significativo, quebra de sigilo financeiro dos clientes de forma massiva ou acesso direto a informações consideradas críticas.
- **Alto (Impacto Significativo)** – Incidentes com potencial de degradação observável dos principais serviços e processos críticos com o potencial de afetar o valor ou a reputação organizacional. Quebra de sigilo financeiro dos clientes de forma isolada ou acesso direto a informações consideradas restritas
- **Médio (Impacto Mensurável)** – Incidente com potencial de impacto nas operações e processos críticos, mas o risco de afetar valor ou reputação organizacional é considerado baixo. Evento que caso não tenha o devido tratamento pode evoluir para situação de risco elevado.

Com base na classificação, deve ser definido um plano de comunicação, considerando que para casos de médio risco que não envolvam terceiros ou clientes, apenas a área de TI e o gestor responsável pelo recurso ou informação devem ser comunicados, enquanto para casos de maior impacto será formado um comitê interno para implementação do plano de ação, composto pelas áreas de TI, Jurídico, *Compliance* e pela Diretoria Executiva, além de outros departamentos, conforme cada caso.

6.2. Plano de Comunicação

Além da previsão expressa de comunicação interna do incidente mediante abertura de chamados e envio de e-mail à área de TI, conforme disposto anteriormente, quando o incidente envolver: (i) outras instituições; (ii) clientes; e/ou (iii) vazamentos de informações sigilosas e/ou confidenciais, a WHG notificará os respectivos indivíduos afetados via e-mail, com vistas que as ações necessárias sejam

tomadas. Essa comunicação deverá conter, no mínimo, informações sobre o incidente e o plano de ação da WHG para minimizar o impacto.

Em conformidade com a regulamentação em vigor, adicionalmente aos meios de comunicação internamente definidos, em caso de incidentes que configurem uma situação de crise, a WHG comunicará tempestivamente o Banco Central acerca de sua ocorrência e as providências para o reestabelecimento das atividades.

7. Conscientização e Treinamento

A WHG se compromete com a contínua conscientização de seus Colaboradores, diante da relevância do tema tratado na presente Política, divulgando informativos sobre os riscos e práticas de segurança da informação, visando mitigar e evitar vulnerabilidades. O objetivo dos informativos é alertar, dar transparência e orientar na atuação dos Colaboradores da WHG.

Além disso, conforme estabelecido na Política de Treinamentos, os Colaboradores da WHG devem receber treinamento periódico sobre Segurança da Informação e Segurança Cibernética, de acordo com adequação e relevância para as habilidades, responsabilidades e funções de cada profissional.

8. Relatório Anual

A WHG elaborará relatório anual sobre a implementação da presente política, com data-base de 31 de dezembro, contento no mínimo:

I - a efetividade da implementação das ações a serem desenvolvidas para adequar as estruturas organizacional e operacional aos princípios e às diretrizes desta Política;

II - o resumo dos resultados obtidos na implementação das rotinas, dos procedimentos, dos controles e das tecnologias a serem utilizados na prevenção e na resposta a incidentes;

III - os incidentes relevantes relacionados com o ambiente cibernético ocorridos no período; e

IV - os resultados dos testes de continuidade de negócios, considerando cenários de indisponibilidade ocasionada por incidentes.

O relatório mencionado deverá ser submetido ao *Compliance,* e, apresentado à Diretoria Executiva até 31 de março do ano seguinte ao da data-base (31 de dezembro).

9. Glossário

Segurança da Informação – Conjunto de medidas e tecnologias empregadas na preservação das propriedades das informações, tais como a confidencialidade, disponibilidade e integridade.

Confidencialidade – Práticas voltadas para a preservação das restrições de autorização de acesso a informações e controles para sua divulgação, incluindo os meios para proteger a privacidade individual e as informações de uso exclusivos.

Disponibilidade – Práticas para garantir que as informações estejam acessíveis e seu uso seja realizado de modo confiável e tempestivo.

Integridade – Práticas de segurança contra a alteração ou destruição inapropriada e não autorizada de informações, o que inclui assegurar o não repúdio e a exatidão das informações.

***Need-to-know / need-to-have* –** Princípio que determina que os dados sejam acessados apenas por pessoas autorizadas, que tenham necessidades específicas de saber para desempenho de suas funções.

Active Directory – Serviço de diretórios da rede Microsoft, utilizado para autenticação e registro de usuários.

Segurança Cibernética – Conjunto de medidas e tecnologias empregadas na defesa dos sistemas de informação, infraestrutura, rede de computadores e/ou dispositivos pessoais, com o objetivo de prevenir danos, roubos, intrusão ou destruição de informações através de ataques cibernéticos.

Incidentes de Segurança – Violação ou ameaça iminente de violação de políticas de segurança digital, políticas de uso aceitável ou práticas de segurança comuns.

Anti-spam – Tecnologia que observa, categoriza, filtra e elimina e-mails com conteúdo impróprio, vírus, propaganda e tipos de mensagens que não sejam autorizadas pela organização.

DDoS (distributed denial of services) – ataques visando negar ou atrasar o acesso aos serviços ou sistemas.

Botnets – ataques que ocorrem de muitos computadores infectados, utilizados para criar e mandar *spam* ou vírus, ou inundar uma rede com mensagens resultando na negação de serviços.

Malware – *Softwares* desenvolvidos para corromper computadores e redes. Exemplos tradicionais de códigos maliciosos incluem vírus, *cavalo de troia, spyware e ramsomware.*

Phishing – *Links* transmitidos por e-mails, simulando ser uma pessoa ou empresa confiável, para obter informações confidenciais;

Backup – Ação de copiar dados de um sistema ou ambiente de produção para um ambiente paralelo com o objetivo de permitir a recuperação dos dados.

Nuvem (*Cloud*) – Fornecimento de recursos externos de tecnologia que possibilita o armazenamento, processamento e troca de informações. Os dados inseridos na Nuvem são acessíveis a dispositivos conectados à Internet que tenham usuário e senha válidos.

10. Vigência e Atualização

Esta Política será revisada anualmente, e sua alteração acontecerá caso seja constatada necessidade de atualização do seu conteúdo. Poderá, ainda, ser alterada a qualquer tempo em razão de circunstâncias que demandem tal providência.

Controle de versões	Data	Modificado por	Descrição da mudança
1.0	Outubro/2020	*Compliance*	Versão inicial
2.0	Junho/2021	*Legal & Compliance* TI	Revisão
3.0	Setembro/2022	*Legal & Compliance* TI	Revisão
4.0.	Novembro/2022	*Legal & Compliance* TI	Revisão
5.0	Dezembro/2023	*Legal & Compliance* TI – Segurança de Informação	Revisão