Política de Segurança da Informação, Segurança Cibernética e Proteção de Dados

Versão vigente: Junho/2026

Versão anterior: Setembro/2023

Sumário

I. Apresentação 3
II. Proteção de Dados Pessoais 3
III. Procedimentos de Segurança da Informação 7
III.A. Acesso Restrito 7
III.B. Sistema de arquivos e Back-up 8
III.C. Cópia de Arquivos e Instalações 9
III.D. Descarte de Informações 9
III.E. Redundância 10
IV. Suporte e Monitoramento 10
IV.A. Tratamento de Casos de Vazamento de Informações Confidenciais 11
IV.B. Firewall 11
IV.C. Rede Wireless 11
IV.D. Testes de Segurança 12
V. Identificação e Avaliação de Riscos Cibernéticos 12
VI. Ações de Proteção e Prevenção aos Riscos Cibernéticos 12
VII. Mecanismos de Supervisão da Segurança Cibernética 14
VIII. Respostas a Incidentes Cibernéticos 14
IX. Programa de Treinamento 15
X. Disposições Gerais e *Enforcement* 15
XI. Vigência, Atualização e Disposições Finais 16

I. APRESENTAÇÃO

Esta Política de Segurança da Informação, Segurança Cibernética e Proteção de Dados ("Política") da **Milênio Capital Gestão de Investimentos Ltda.** ("Milenio") tem por objetivo precípuo a definição de regras e princípios norteadores das condutas dos colaboradores da Milenio, assim entendidos seus (i) sócios, (ii) funcionários, (iii) diretores, (iv) estagiários, ou (v) quaisquer pessoas que, em virtude de seus cargos, funções ou posições na Milenio, tenham acesso a informações confidenciais sobre a Milenio, seus negócios, clientes ou investidores ou, ainda, aqueles que participem do processo de decisão de investimentos, em especial no que se refere à segurança da informação, segurança cibernética e proteção de dados.

Os colaboradores atestam a ciência e adesão acerca dos procedimentos definidos pela presente Política mediante assinatura de termo próprio, sendo submetidos anualmente ao Programa de Treinamento adotado pela Milenio, a fim de que sejam orientados sobre as rotinas a serem observadas no desempenho dos processos descritos nesta Política.

A Milenio coletará Termo de Confidencialidade de quaisquer terceiros contratados que tiverem acesso às informações confidenciais a respeito da Milenio, seus colaboradores, fundos sob gestão e investidores, salvo se este compromisso já tiver sido assumido pelo terceiro mediante a assinatura de instrumento apartado.

Em caso de dúvidas ou necessidade de aconselhamento, o colaborador deve buscar auxílio junto à Diretora de Compliance da Milenio, devendo as questões de segurança cibernética serem tratadas com o responsável pela Tecnologia da Informação.

II. PROTEÇÃO DE DADOS PESSOAIS

O presente Capítulo visa regular o tratamento de Dados Pessoais e Dados Pessoais Sensíveis pela Milenio, assim considerada toda operação realizada com tais dados, como as que se referem à coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Considera-se "Dados Pessoais" qualquer informação relacionada a pessoa natural identificada ou identificável. Deste modo, sujeitam-se à tutela desta Política todos os Dados Pessoais de colaboradores, investidores, parceiros, prestadores de serviço ou quaisquer terceiros com os quais a Milenio mantenha relacionamento de qualquer natureza.

São considerados, ainda, Dados Pessoais aqueles utilizados para formação de perfil comportamental de determinada pessoa natural, se identificada.

Consideram-se "Dados Pessoais Sensíveis" os Dados Pessoais que versem sobre a origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculados a uma pessoa natural.

Todos os Dados Pessoais ou Dados Pessoais Sensíveis são informações confidenciais e devem ser tratados como tal para os fins desta Política e demais manuais e políticas internas adotadas pela Milenio.

As atividades de tratamento de Dados Pessoais e Dados Pessoais Sensíveis deverão observar a boa-fé e os seguintes princípios:

a) finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
b) adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
c) necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
d) livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus Dados Pessoais;
e) qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
f) transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
g) segurança: utilização de medidas técnicas e administrativas aptas a proteger os Dados Pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
h) prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de Dados Pessoais;
i) não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
j) responsabilização e prestação de contas: demonstração, pela Milenio, da adoção de medidas eficazes

e capazes de comprovar a observância e o cumprimento das normas de proteção de Dados Pessoais e, inclusive, da eficácia dessas medidas.

O tratamento de Dados Pessoais e Dados Pessoais Sensíveis pela Milenio só será realizado nas seguintes hipóteses:

a) para o cumprimento de obrigação legal ou regulatória pela Milenio;
b) quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
c) quando necessário para atender aos interesses legítimos da Milenio ou de terceiros, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos Dados Pessoais e Dados Pessoais Sensíveis;
d) mediante o fornecimento de consentimento pelo titular por escrito ou outro meio que demonstre a manifestação de vontade do titular; ou
e) para o exercício regular de direitos em processo judicial, administrativo ou arbitral.

O legítimo interesse da Milenio indicado no item "c" acima poderá ter fundamento, mas não se limita, às seguintes finalidades:

i) apoio e promoção de atividades da Milenio;
ii) proteção, em relação ao titular, do exercício regular dos seus direitos ou prestação de serviços que o beneficie, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais.

No caso de interesse legítimo da Milenio, somente os Dados Pessoais e Dados Pessoais Sensíveis estritamente necessários serão tratados, sendo outorgada ampla transparência ao titular sobre o tratamento implementado.

O consentimento de que trata o item "d" acima deve observar as seguintes diretrizes:

a) se outorgado por escrito deverá constar de cláusula destacada das demais cláusulas contratuais;
b) o Dado Pessoal obtido mediante consentimento do titular só poderá ser compartilhado com terceiros se houver expressa autorização do titular nesse sentido;
c) o consentimento deve referir-se a finalidades determinadas, sendo nulas as autorizações genéricas para o tratamento de dados. Caso alterada a finalidade, deverá ser coletado novo consentimento do titular; e
d) o consentimento poderá ser revogado a qualquer tempo por manifestação expressa do titular, por procedimento gratuito e facilitado, ratificado o tratamento realizado ao amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação dos dados.

A Milenio outorgará ao titular o direito ao acesso facilitado às informações sobre o tratamento de seus dados, que serão disponibilizadas de forma clara, adequada e ostensiva, incluindo as seguintes informações:

a) finalidade específica do tratamento, ratificando que o tratamento de Dados Pessoais é condição para o fornecimento do serviço de gestão profissional de recursos em virtude de obrigação regulatória;
b) forma e duração do tratamento, observados os segredos comercial e industrial;
c) identificação e informações de contato da Milenio que atuará como controladora da informação;
d) informações acerca do potencial compartilhamento de dados pela Milenio e a sua finalidade;
e) responsabilidades dos colaboradores que realizarão o tratamento; e
f) informações sobre os direitos do titular, na forma do art. 18 da Lei Geral de Proteção de Dados, e meios pelos quais tais direitos poderão ser exercidos.

O término do tratamento de Dados Pessoais e Dados Pessoais Sensíveis ocorrerá nas seguintes hipóteses:

a) verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada;
b) fim do período de tratamento, ou seja, 05 (cinco) anos após a cessação da prestação de serviço ao titular;
c) comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento, resguardado o interesse público; ou
d) determinação da autoridade nacional, quando houver violação da Lei Geral de Proteção de Dados.

Os Dados Pessoais e Dados Pessoais Sensíveis serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades:

a) cumprimento de obrigação legal ou regulatória pela Milenio;
b) transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos acima; ou
c) uso exclusivo da Milenio, vedado seu acesso por terceiro, e desde que anonimizados os dados.

A Milenio manterá registro das operações de tratamento de Dados Pessoais e Dados Pessoais Sensíveis que realizar, especialmente quando baseado no seu legítimo interesse.

O encarregado pelo tratamento de Dados Pessoais e Dados Pessoais Sensíveis é o *Chief Technology Officer* (CTO) da Milenio, estando as informações para contato disponíveis no site da gestora.

III. PROCEDIMENTOS DE SEGURANÇA DA INFORMAÇÃO

III.A. ACESSO RESTRITO

A troca de informações entre os colaboradores da Milenio deve sempre pautar-se no conceito de que o receptor deve ser alguém que necessita receber tais informações para o desempenho de suas atividades e que não está sujeito a nenhuma barreira que impeça o recebimento daquela informação. Em caso de dúvida a área de Compliance será acionada previamente à revelação.

Os colaboradores da Milenio que tiverem acesso aos sistemas de informação serão responsáveis por tomar as precauções necessárias de forma a impedir o acesso não autorizado aos sistemas, devendo salvaguardar as senhas e outros meios de acesso aos mesmos.

O acesso controlado às pastas e arquivos se dá mediante a outorga de senhas de acesso individuais e intransferíveis, seguindo o princípio do privilégio mínimo, que permitem a identificação do seu usuário, afastando a utilização das informações ali contidas por pessoas não autorizadas.

O administrador de TI da Milenio deve realizar uma análise de todas as permissões de acesso, à rede ou a outros dispositivos pelos quais é responsável, pelo menos 01 (uma) vez a cada 6 (seis) meses. Esta ação deve confirmar positivamente todos os usuários atuais. Todas as contas de usuários, que não podem ser identificadas como ativas, serão desativadas imediatamente, ficando pendente de exclusão.

Adicionalmente, todas as mensagens enviadas/recebidas dos computadores disponibilizados pela Milenio permitem a identificação do seu remetente/receptor.

A outorga e cancelamento de senhas é de responsabilidade do TI, sempre mediante orientação da Diretora de Compliance e/ou do *Chief Technology Officer* (CTO), a quem compete a verificação das estruturas de governança e tecnológica da Milenio, respectivamente, a fim de evitar a transgressão de barreiras de informação e potenciais conflitos de interesse. Este procedimento deverá ser observado ainda na hipótese de mudança de atividade e/ou de área de um determinado profissional dentro da Milenio.

As senhas de acesso, que devem ser mantidas confidenciais e são de responsabilidade do respectivo colaborador, possuem prazo de validade e requisitos mínimos de segurança, sendo desabilitadas após um número máximo de tentativas malsucedidas de acesso, sendo esta atividade registrada pelos controles de tecnologia da informação.

Após um tempo máximo de inatividade, a sessão dos sistemas internos e dispositivos fornecidos pela Milenio

é encerrada, voltando para uma tela protegida por senha que exige uma nova autenticação para que o usuário retome suas atividades normalmente.

No caso do desligamento ou saída de algum colaborador, o acesso aos sistemas e arquivos será automaticamente revogado pelo bloqueio de login do usuário e invalidação de todas as sessões ativas, juntamente com a modificação da respectiva senha. Para sistemas externos, a Milenio submeterá uma solicitação de revogação de acesso imediatamente e assegurar-se de que os acessos sejam revogados.

III.B. Sistema de arquivos e Back-up

Todos os arquivos utilizados pela Milenio no desempenho de suas atividades devem ser gerenciados e armazenados em um serviço de armazenamento em nuvem de alta qualidade, reconhecido pela sua robustez, confidencialidade e confiabilidade. Esse serviço deve cumprir, no mínimo, os seguintes requisitos:

- Garantia de Alta Disponibilidade: O serviço de armazenamento em nuvem selecionado deve garantir alta disponibilidade dos dados, assegurando que os arquivos estejam acessíveis sempre que necessário.
- Replicação e Back-up Automático: O serviço de armazenamento deve realizar automaticamente a replicação e back-up dos dados. Esta é uma medida essencial para prevenir a perda de informações.
- Controle de Permissões de Acesso: Deve ser implementada uma política de permissões de acesso detalhada. Apenas indivíduos autorizados poderão acessar arquivos e documentos específicos.
- Registro de Acesso e Modificação: Todas as ações de acesso ou modificação devem ser monitoradas e registradas. Essa medida visa manter a responsabilidade e rastrear possíveis falhas de segurança.
- Versionamento de Arquivos: O serviço de armazenamento em nuvem deve permitir o versionamento de arquivos. Isso permite que as versões anteriores de arquivos e documentos possam ser acessadas e restauradas, se necessário.
- Aplicação Cliente para Windows: O serviço deve disponibilizar uma aplicação cliente compatível com o sistema operacional Windows. Esta aplicação deverá manter os documentos sincronizados entre todas as máquinas, garantindo que todos os usuários tenham sempre acesso à versão mais atualizada de cada arquivo.

Ainda, todos os sistemas internos devem:

- Definição de Rotina Automática de Backup: Todos os sistemas internos da empresa devem implementar uma rotina automática de back-up dos dados. Essa medida é essencial para garantir a preservação e recuperação dos dados, caso seja necessário.
- Frequência e Janela de Retenção de Back-up: A frequência e a janela de retenção dos back-ups devem ser definidas de acordo com o tipo de dado armazenado. Cada sistema interno deve avaliar a

criticidade de suas informações e ajustar a frequência de back-ups e o período de retenção para garantir que os dados possam ser recuperados adequadamente em caso de perda.

- Rotina de Restauração de Dados: É essencial garantir a eficácia dos back-ups através de uma rotina de teste de restauração. Tal rotina deve ser cumprida regularmente para garantir que os dados possam ser restaurados a partir dos back-ups, caso necessário.
- Rotina de Replicação de Dados: Além do back-up, todos os sistemas internos devem implementar uma rotina de replicação de dados. Essa rotina deve garantir a cópia segura dos dados para um local/ambiente separado, fornecendo uma proteção adicional em caso de falha de sistema ou situação de contingência.
- Garantia de Segurança dos Dados: As rotinas de back-up e replicação devem ser realizadas de forma a garantir a segurança dos dados, prevenindo o acesso não autorizado durante o processo.

Estas diretrizes asseguram a integridade, a confidencialidade e a disponibilidade de todos os dados e informações gerenciados pela Milenio.

III.C. Cópia de Arquivos e Instalações

Todos os sistemas e programas de computador utilizados pelos colaboradores devem ter sido previamente autorizados pelo CTO. Downloads de qualquer natureza podem ser realizados, desde que de forma justificada.

A cópia de arquivos e instalação de programas em computadores respeitará os direitos de propriedade intelectual pertinentes, tais como licenças e patentes.

É terminantemente proibido que os colaboradores façam cópias (físicas ou eletrônicas) ou imprimam os arquivos utilizados, gerados ou disponíveis na rede e circulem em ambientes externos com estes arquivos, salvo se em prol da execução e do desenvolvimento dos negócios e dos interesses da Milenio. Nestes casos, o colaborador que estiver na posse e guarda do arquivo será o responsável direto por sua boa conservação, integridade e manutenção de sua confidencialidade.

Qualquer impressão de documentos deve ser imediatamente retirada da máquina impressora, pois pode conter informações restritas e confidenciais mesmo no ambiente interno da Milenio. É vedada, ainda, a manutenção destes em mesas, máquinas de fax ou copiadoras.

III.D. Descarte de Informações

O descarte de informações confidenciais deve observar as seguintes diretrizes:

a) o conteúdo descartado deverá ser apagado e/ou as mídias devem ser destruídas, impossibilitando a sua recuperação, de modo que a informação não fique vulnerável a acesso não autorizado;
b) os documentos físicos que contenham informação protegida devem ser triturados imediatamente após seu uso de maneira a evitar sua recuperação ou leitura;
c) a eliminação ou a destruição final das mídias ou documentos, realizada por terceiros, deve ser documentada;
d) dispositivos de memória e dispositivos de armazenamento (por exemplo laptops, dispositivos USB, discos rígidos portáteis, tablets, smartphones) desativados pela Milenio devem ser apagados de modo que a informação protegida que neles havia seja irrecuperável.

III.E. Redundância

Além das cópias de segurança acima, outros recursos de TI são redundantes. Em caso de pane e indisponibilidade de acesso físico ao local de trabalho, a equipe poderá acessar as informações na nuvem, adotando-se o mesmo protocolo de home office (trabalho remoto) utilizado por parte dos colaboradores da Milenio.

Para garantir o funcionamento da rede e a integridade dos dados, mesmo na eventual interrupção do fornecimento de energia elétrica, todas as estações de trabalho e a infraestrutura de rede estão conectados a um equipamento do tipo *no-break*, que permite a continuidade do funcionamento da rede por tempo suficiente para que os usuários salvem seus arquivos, evitando perda de trabalho e corrupção dos dados.

IV. Suporte e Monitoramento

Em caso de pane da rede ou em alguma estação de trabalho, o fato deverá ser imediatamente comunicado à área de TI, que assegurará o suporte interno ou providenciará que seja acionado o suporte externo, caso necessário.

Os sistemas e dispositivos eletrônicos utilizados pela Milenio estão sujeitos à revisão e monitoramento a qualquer época sem aviso ou permissão, de forma a detectar qualquer irregularidade na transferência de informações, seja interna ou externamente.

Nesse sentido, tendo em vista que a utilização do e-mail se destina exclusivamente para fins profissionais, como ferramenta para o desempenho das atividades dos colaboradores, a Milenio também poderá monitorar toda e qualquer troca, interna ou externa, de e-mails dos colaboradores.

Qualquer suspeita ou conhecimento de violação desta Política ou incidente de segurança da informação deve

ser objeto de informação ao CTO e à Diretora de Compliance para que sejam tomadas as devidas providências com relação à apuração dos fatos, mitigação de eventuais riscos, implementação de procedimentos corretivos e responsabilização dos envolvidos.

Periodicamente e sem aviso prévio, poderão ser realizadas inspeções nos computadores para fins de monitoramento e averiguação de conformidade das atividades operacionais, incluindo downloads impróprios, não autorizados ou gravados em locais indevidos.

IV.A. Tratamento de Casos de Vazamento de Informações Confidenciais

No caso de vazamento de informações confidenciais relacionadas a investidores, contrapartes, ou de qualquer outro Dado Pessoal ou Dado Pessoal Sensível tratado pela Milenio, ainda que oriundo de ação involuntária, a Diretora de Compliance notificará os interessados sobre o ocorrido.

Sem prejuízo, a Milenio acionará o seu Plano de Recuperação visando a identificação da causa que ensejou o vazamento e responsabilização do causador, se for o caso. Ademais, será elaborado um relatório acerca dos danos ocorridos, percentual das atividades afetadas, impactos financeiros, sugerindo ainda medidas a serem tomadas de modo a possibilitar que as atividades voltem a ser executadas normalmente.

Este relatório será elaborado pela Diretora de Compliance e será submetido à Diretoria da Milenio que promoverá as iniciativas cabíveis para o retorno à normalidade com a maior brevidade possível.

IV.B. Firewall

A Milenio faz o uso da tecnologia de Firewall para proteger sua rede contra ameaças externas. De modo automático, o Firewall realiza o bloqueio de sites que são reconhecidos como de alto risco, a fim de evitar a propagação de vírus corporativo e acesso a materiais não condizentes com a atuação da Milenio, tais como: (i) adulto; (ii) sexual; (iii) jogos e apostas; (iv) ofensivos; (v) atividade criminal; (vi) armas; (vii) fraude; (viii) drogas; e (ix) relacionamento.

IV.C. Rede Wireless

A Milenio possui 2 (duas) redes Wi-Fi distintas, uma para uso interno e outra para uso dos visitantes. A senha de acesso às redes jamais deve ser divulgada para visitantes. Os visitantes devem sempre solicitar a senha de acesso para a recepcionista.

A rede Wi-Fi para visitantes é bloqueada para acessar recursos internos.

IV.D. Testes de Segurança

São realizados os seguintes testes de segurança para monitoramento dos sistemas utilizados:

ROTINAS OPERACIONAIS	PERIODICIDADE
Varredura de antivírus	Tempo real
Controle de conteúdo de Internet pelo Firewall e Antivírus	Tempo real
Varredura de memória pelo Antivírus	Tempo real
Monitoramento de Hosts e serviços	Tempo real
Autenticação de rede	Tempo real
Bloqueio de tela do Windows por Inatividade	A cada 15 min
Back-up Online	Tempo real
Back-up Firewall	Semanal
Verificar status dos logs do Back-up	Sob demanda
Verificar sistema gráficos de consumo de link, visão diária, semanal e mensal	Diário
Teste de restore do back-up	Anual
Verificar status Nobreak CPD Gerenciável	Anual
Atualizar plano de ação	Anual
Atualizações Microsoft nas estações de trabalho	Semanal
Atualizar do Firmware de Firewall	Sob demanda
Troca da senha dos usuários	180 dias

V. Identificação e Avaliação de Riscos Cibernéticos

Considerando a atividade de gestão profissional de recursos de terceiros desempenhada pela Milenio, são essenciais todos os recursos tecnológicos necessários ao processo de análise, investimento e desinvestimento, tais como: (i) compra e venda de ativos para as carteiras sob gestão; (ii) conferência e liberação das carteiras; e (iii) acesso aos sistemas de informação.

Diante da possibilidade de invasores utilizarem (i) *Malware*, (ii) Engenharia social; (iii) *Pharming*; (iv) *Phishing*; (v) *Vishing*; (vi) *Smishing*; (vii) Acesso pessoal; (viii) Ataques de DDos (*distributed denial of services*) e *botnets*; e (ix) Invasões (*advanced persistent threats*), a Milenio adota ações de prevenção e proteção, nos termos do capítulo seguinte.

VI. Ações de Proteção e Prevenção aos Riscos Cibernéticos

Os planos de ação e prevenção descritos neste capítulo tem por objetivo mitigar e minimizar a possibilidade de ocorrência de um ataque cibernético, na tentativa de evitar que os riscos identificados se concretizem.

Neste sentido, a Milenio ratifica a adoção de controles de acesso físico e lógico implementados em linha com

a presente Política. Tais controles visam a identificação, autenticação e autorização de acesso pelos usuários a sistemas ou ativos da Milenio, evitando o acesso por terceiros não autorizados.

Isto posto, todos os colaboradores devem observar de forma estrita as rotinas relacionadas à definição de senhas de acesso aos sistemas e rede.

Os eventos de login e alteração de senhas são rastreáveis e auditáveis, sendo qualquer inconsistência ou inadequação com relação aos acessos recomendados pela Diretora de Compliance reportados imediatamente. Especial atenção deverá ser envidada aos casos de desligamento ou gozo de férias de colaboradores.

São adotadas as seguintes medidas preventivas para cada risco identificado:

Risco Externo	Ação de Proteção/Prevenção
Tentativa de invasão à rede interna	O *firewall* instalado na rede analisa todo o tráfego de entrada na rede. Caso um dos acessos seja suspeito, o próprio *firewall* realiza o bloqueio, de forma proativa.

Risco Interno	Ação de Proteção/Prevenção
Indisponibilidade dos arquivos na rede	Uso de sistemas com redundância interna para garantir alta disponibilidade e robustez operacional (*Sharepoint*).
Possibilitar acessos indevidos às aplicações restritas da empresa	Troca periódica das senhas cadastradas com alto nível de criticidade e segurança; uso obrigatório de MFA em todas as aplicações/serviços; Trilha de auditoria habilitada.
Perda de arquivos de usuários	*Backup* em nuvem de todos os dados que estão no servidor.

Todos os novos equipamentos e sistema instalados na Milenio devem contar com as configurações de proteção acima descritas, assegurada através de políticas do domínio Microsoft, sendo realizado teste em ambientes de homologação e de prova antes do início da sua utilização. Adicionalmente, são realizadas inspeções com periodicidade semanal visando a verificação da atualização dos sistemas operacionais e softwares instalados nos computadores da Milenio.

Todos os programas de computador utilizados pelos colaboradores devem ter sido previamente autorizados pelo CTO, sendo vedadas aplicações não autorizadas por meio de controles de execução de processos. Downloads de qualquer natureza podem ser realizados, desde que de forma justificada.

VII. MECANISMOS DE SUPERVISÃO DA SEGURANÇA CIBERNÉTICA

A Milenio realiza testes de segurança para confirmar e validar que: (i) existe inventários atualizados de hardware e software, verificando com frequência para identificar elementos estranhos à Milenio, como por exemplo, computadores não autorizados ou software não licenciado; (ii) os sistemas operacionais e softwares de aplicação estão atualizados, instalando as atualizações sempre que forem disponibilizadas; (iii) estão sendo realizadas as rotinas de back-up, executando testes regulares de restauração de dados; (iv) os logs dos colaboradores estão devidamente ativos; (v) a rotina de alteração periódica de senha de acesso está sendo cumprida; e (vi) está sendo assegurada a segregação de acessos.

São mantidos inventários atualizados de hardware e softwares utilizados pela Milenio. Em tempo real são realizadas verificações, a fim de identificar elementos estranhos à Milenio, tais como computadores não autorizados ou softwares não licenciados.

Sempre que houver alteração relevante na estrutura tecnológica da Milenio serão realizadas análises de vulnerabilidade.

VIII. RESPOSTAS A INCIDENTES CIBERNÉTICOS

Compete à Diretora de Compliance da Milenio a comunicação do incidente aos demais colaboradores da Milenio, orientando-os sobre a postura e providências cabíveis, de acordo com a natureza e severidade da contingência, em observância do Plano de Continuidade de Negócios.

Para os fins desta Política, bem como do Plano de Continuidade de Negócios, incidente pode ser considerado todo evento ou ação que comprometeu ou pode comprometer a confidencialidade, integridade ou disponibilidade de informações confidenciais e/ou de Dados Pessoais, incluindo, mas não se limitando a: (a) perda ou roubo de materiais ou equipamentos, por exemplo, notebooks; (b) divulgação de dados pessoais para destinatário incorreto; (c) falha dos sistemas adotados pela Milenio; (d) tentativas (bem sucedidas ou não) de acesso ou divulgação não autorizada de informações confidenciais e/ou de Dados Pessoais; (e) ataques (bem sucedidos ou não) de *hackers*; (f) circunstâncias imprevistas, como incêndio.

Cabe à Diretora de Compliance, junto ao CTO, desenvolver relatórios acerca dos danos ocorridos, percentual das atividades afetadas, os tipos de dados e/ou informações que foram ou podem ter sido violados, as proteções que estão em vigor, o que aconteceu com os dados e/ou informações após o incidente, os titulares dos dados e/ou informações que foram afetados, o número de titulares afetados, os prejuízos potenciais aos titulares, possíveis impactos financeiros, sugerindo ainda medidas a serem tomadas de modo a possibilitar

que as atividades voltem a ser executadas normalmente. Tais relatórios deverão ser submetidos à Diretoria da Milenio que promoverá as iniciativas cabíveis para o retorno à normalidade com a maior brevidade possível.

Após a conclusão do gerenciamento do incidente, caso seja identificada a causa e o responsável por este, a Diretora de Compliance tomará as providências cabíveis para responsabilização dos envolvidos, estando os colaboradores da Milenio sujeitos às penalidades previstas em seus manuais e políticas internas de *compliance*, bem como às penalidades prevista em lei.

IX. PROGRAMA DE TREINAMENTO

A Milenio conta com um programa de treinamento dos colaboradores que tenham acesso a informações confidenciais, na forma descrita em seu Código de Ética e Conduta. O treinamento levará em consideração o tratamento das informações confidenciais e, no que se refere ao tratamento de Dados Pessoais e Dados Pessoais Sensíveis, abordará aspectos como: (i) natureza; (ii) escopo; (iii) finalidade; (iv) probabilidade e a gravidade de riscos; e (v) benefícios decorrentes do tratamento de dados.

Os procedimentos e rotinas definidos na presente Política serão abordados em treinamento anual, coordenado pela Diretora de Compliance ou terceiro contratado para esta finalidade, visando a sua disseminação entre a equipe da Milenio.

Poderão ser promovidos treinamentos em periodicidade menor, visando a atualização e ampliação do conhecimento dos colaboradores, em especial em virtude de mudanças relevantes nos procedimentos e controles descritos nesta Política.

X. DISPOSIÇÕES GERAIS E *ENFORCEMENT*

Todos os documentos, relatórios e informações relevantes para os procedimentos e rotinas descritos nesta Política são arquivados em meio físico ou eletrônico na Milenio, pelo prazo mínimo de 5 (cinco) anos.

Esta Política prevalece sobre quaisquer entendimentos orais ou escritos anteriores, obrigando os colaboradores da Milenio aos seus termos e condições.

A título de *enforcement*, vale notar que a não observância dos dispositivos da presente Política resultará em advertência, suspensão, demissão ou exclusão por justa causa, conforme a gravidade e a reincidência na violação, sem prejuízo das penalidades civis e criminais.

XI. VIGÊNCIA, ATUALIZAÇÃO E DISPOSIÇÕES FINAIS

A presente Política será revisada, no mínimo, a cada 2 (dois) anos, 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.

Esta Política é parte integrante das políticas internas da Milenio, e estará disponível para consulta em sua sede.