POLÍTICA DE SEGURANÇA CIBERNÉTICA E DA INFORMAÇÃO

Versão	Motivo da Alteração	Data	Autor/Revisor	Aprovado por:	Data de Aprovação
1.0	Atualização	Agosto/2021	Rafael Kochi	Alexandre Despontin	Outubro/21

SUMÁRIO

Introdução

A presente **Política de Segurança Cibernética e da Informação** ("**Política**") busca atender à demanda regulatória da **Mérito Distribuidora de Títulos e Valores Mobiliários Ltda.**, sociedade limitada inscrita no CNPJ/ME sob o número 41.592.532/0001-42, e **Mérito Investimentos S.A,** sociedade anônima inscrita no CNPJ/ME sob o número 15.632.652/0001-16, ambas localizadas na cidade de São Paulo, Estado de São Paulo na Rua Funchal, nº418, 21º andar, Vila Olímpia, CEP 04551-060 ("**Mérito DTVM**" e "**Mérito Investimentos**, respectivamente, sendo em conjunto como "**Grupo Mérito**"), e terá abaixo descrito acerca das políticas e manuais que são aplicáveis e estabelecidas pelo Grupo Mérito, com o objetivo de determinar as regras que orientam a conduta, processos e fluxos a serem seguidos por parte de todos os diretores, empregados e prestadores de serviços ("**Colaborador**" ou, em conjunto, "**Colaboradores**") do Grupo Mérito.

1. Conceitos Aplicáveis.

- **Administradores**: São os membros da Diretoria.
- **Coligadas:** As sociedades em que a os sócios comuns tenham influência significativa (art. 243, §1º, da Lei nº 6.404/76).
- **Conflito de Interesse**: Situação em que uma pessoa se encontra envolvida em processo decisório cujo resultado tenha o poder de influenciar e/ou direcionar, assegurando um ganho e/ou benefício para si, algum Membro Próximo da Família, sociedade por ele controlada ou terceiro com o qual esteja envolvido, ou ainda esteja em situação que possa interferir na sua capacidade de julgamento isento. Incluem-se nessa definição as situações nas quais os objetivos ou motivações dos tomadores de decisão, por qualquer razão, não estejam alinhados aos objetivos e aos interesses do Grupo Mérito e respectivos acionistas em matérias específicas.
- **CVM**: Comissão de Valores Mobiliários
- **Diretoria**: São as pessoas físicas qualificadas e empossadas nos termos do

contrato social ou estatuto social do Grupo Mérito, conforme aplicável.

- **Grupo Mérito**: É considerado o conjunto das empresas Mérito Investimentos S.A e Mérito Distribuidora de Títulos e Valores Mobiliários Ltda em razão de serem empresas Coligadas.
- **Riscos Cibernéticos**: são os riscos de ataques cibernéticos, oriundos de malware, técnicas de engenharia social, invasões, ataques de rede (DDoS e Botnets), fraudes externas, entre outros, que possam expor Dados, redes e sistemas do Grupo Mérito, causando danos financeiros e/ou de reputação consideráveis, podendo, em algumas circunstâncias, prejudicar a continuidade das atividades.
- **Serviços Relevantes**: Serviços prestados por Prestadores de Serviço ao Grupo Mérito cuja indisponibilidade, vulnerabilidade ou inconsistência possa prejudicar a continuidade de seus negócios: (i) afetando o atendimento ofertado ao Cliente; (ii) paralisando a operação de empresa do Grupo Mérito, podendo causar perdas financeiras; ou (iii) impedindo o fornecimento de informações por empresa do Grupo Mérito aos entes reguladores e/ou o cumprimento de direitos e garantias dos clientes.
- **Incidentes:** Qualquer ocorrência que realmente ou potencialmente comprometa a confidencialidade, integridade ou disponibilidade de um sistema de informação ou a informação que o sistema processa, armazena ou transmite ou que constitui uma violação ou ameaça iminente de violação de políticas de segurança, procedimentos de segurança ou políticas de uso aceitáveis. Serão considerados incidentes, mas não se limitando a esses: **(i)** acesso indevido a contas e/ou sistemas do Grupo Mérito; **(ii)** acessos não autorizado a bases de Dados ou Informações de uso interno ou confidencial do Grupo Mérito; **(iii)** alteração ou perda de Dados ou Informações, ou de acesso a sistemas ou ambientes lógicos, bem como da integridade destes; **(iv)** vulnerabilidades existentes nos sistemas, bem como situações de indisponibilidade dos sistemas e/ou das informações ou **(v)** demais falhas de segurança que acarretem em acessos não autorizados a sistemas ou ambientes tecnológicos do Grupo Mérito, por meio de técnicas, conhecimentos e ferramentas para detectar e explorar fragilidades específicas em um ambiente tecnológico.

1.1. Legislação Relacionada.

- Instrução CVM 380 de 23 de dezembro de 2002;
- Instrução CVM 505 de 27 de setembro de 2011, Art. 14; - atualmente Resolução CVM 35 de 27 de maio de 2021
- Resolução CMN 4.557 de 23 de fevereiro de 2017;
- Resolução CMN 2.554 de 29 de setembro de 1998;
- Resolução nº 4.893 de 26 de fevereiro de 2021
- Ofício Circular nº 053 28 de setembro 2012-DP, Itens 2.5.6 e 2.5.7;
- Decreto nº 56.819 de 10 de março de 2011;

2. Vigência, abrangência, revisão e aplicação.

Esta Política entrará em vigor na data de sua aprovação pela Diretoria do Grupo Mérito e permanecerá em vigor por prazo indeterminado. A Política aplica-se a todos os Colaboradores. Qualquer alteração ou revisão desta Política deverá ser submetida a Diretoria, que poderá alterá-la:

(i) em função de modificação nas normas legais e regulamentares aplicáveis, de forma a implementar as adaptações que forem necessárias;

(ii) quando a Diretoria, no processo de avaliação da eficácia dos procedimentos adotados, constatar a necessidade de alterações; e

(iii) devido a revisão periódica, obrigatória, conforme a norma ou “ad hoc” pelo Departamento de Compliance.

Todos os Colaboradores deverão zelar, individualmente, pelo cumprimento do disposto nesta Política, além de observar os códigos e manuais eventualmente aprovados ou aderido, inclusive assumindo o compromisso de informar a Diretoria caso tenha

conhecimento ou suspeita de que a presente Política e demais regulamentações, códigos de autorregulamentação e manuais aos quais o Grupo Mérito se sujeite tenham sido infringidos, em todo ou em parte, por qualquer Colaborador.

3. Da Segurança da Informação.

A política de segurança da informação do Grupo Mérito, tem como objetivo estabelecer regras que orientem o controle de acesso a informações confidenciais pelos Colaboradores, inclusive através do estabelecimento de regras para a utilização de equipamentos e e-mails de domínio do Grupo Mérito, para gravação de cópias de arquivos, para download e instalação de programas nos computadores dentre outras.

Nesse sentido, todos os Colaboradores firmarão o Termo de Adesão anexo à presente Política na forma do "Anexo I", tomando conhecimento e expressamente anuindo com o quanto segue:

(i) Os arquivos físicos com os dados e informações relativas à atividade desenvolvida ficarão alocados em seu respectivo espaço físico. Desta forma, somente os Colaboradores, cujas atividades forem relacionadas com o mercado financeiro e de capitais, terão acesso a informações confidenciais e sigilosas relativas à sua atividade.

(ii) Os equipamentos e computadores disponibilizados aos Colaboradores deverão ser utilizados com a finalidade de atender aos interesses comerciais do Grupo Mérito, não sendo permitida a sua utilização para fins particulares.

(iii) A gravação de cópias de arquivos e instalação de programas em computadores deverá respeitar as regras estabelecidas na presente Política e no Manual de Confidencialidade.

(iv) Downloads de qualquer natureza podem ser realizados, desde que de forma moderada, respeitando o espaço individual de cada usuário. Ocorre que não

será permitido a instalação dos programas sem a aprovação do Departamento de TI. Periodicamente, a critério do Comitê de *Compliance*, poderão ser realizadas inspeções nos computadores para averiguação de downloads impróprios, não autorizados ou gravados em locais indevidos.

(v) O correio eletrônico disponibilizado caracteriza-se como correio eletrônico corporativo para todos os efeitos legais, especialmente os relacionados aos direitos trabalhistas, sendo sua utilização voltada para alcançar os fins comerciais aos quais se destina. É vedado a utilização pessoal.

(vi) As mensagens enviadas ou recebidas por meio de e-mails corporativos, seus respectivos anexos e a navegação por meio da rede mundial de computadores por meio de equipamentos da Grupo Mérito ou dentro das instalações serão ser monitoradas.

(vii) Os e-mails corporativos recebidos pelos Colaboradores, quando abertos, deverão ter seu conteúdo verificado pelo Colaborador, não sendo admitida, sob qualquer hipótese, a manutenção ou arquivamento de mensagens de conteúdo ofensivo, discriminatório, pornográfico ou vexatório, sendo a responsabilidade apurada de forma específica em relação ao destinatário da mensagem. Os arquivos de e-mails corporativos poderão ser inspecionados pelo departamento de Controles Internos, a qualquer tempo e independentemente de prévia notificação.

(viii) Todos os programas de computador utilizados pelos Colaboradores devem ter sido previamente autorizados pelo responsável pelo Departamento de TI Os computadores podem ser inspecionados a qualquer tempo para a verificação da observância do disposto na presente Política.

(ix) Cada um dos Colaboradores, no momento de sua contratação, receberá uma senha secreta, pessoal e intransferível para acesso aos computadores, à rede corporativa e ao correio eletrônico corporativo.

(x) O acesso a informações confidenciais e sigilosas será restrito e poderá ser diferenciado conforme os níveis hierárquicos e as funções desempenhadas pelos Colaboradores conforme previsto no Manual de Segregação de Atividades. O controle de acesso a tais informações será realizado por meio das senhas pessoais dos Colaboradores, que, a critério do Diretoria, poderão alterar e autorizar outra ordem de graduação com diferentes níveis de acessibilidade a arquivos, pastas e diretórios da rede corporativa.

(xi) Cada Colaborador terá acesso a pastas eletrônicas diretamente relacionadas às atividades desenvolvidas pela sua área. Apenas o Departamento de TI e os diretores do Grupo Mérito terão acesso a todas as pastas.

Em complementação aos procedimentos acima, que deverão ser observados por todos os Colaboradores, o Grupo Mérito instalará firewall de segurança nos servidores para acesso à sua rede, visando manter o ambiente de trabalho disponível e livre de vírus e acessos indesejados. O sistema de prevenção a ataques de vírus será atualizado diariamente. O *backup* de arquivos será realizado de forma sistemática com unidade de disco externa e os *links* são dedicados e seguros.

Adicionalmente, o backup de arquivos é feito diariamente e os dados atualizados serão armazenados em local seguro. Novas tecnologias de solução de backup, serão estudadas para futuras implementações, conforme necessidade e desenvolvimento das atividades do Grupo Mérito e orientação do Comitê de Compliance e departamento de Auditoria.

Para garantia e execução das disposições previstas nesta Política, o Departamento de TI utilizará sistemas de terceiro (por exemplo, o sistema PANDA ADPTIVE DEFENSE e ITARIAN), para garantir e executar o monitoramento remoto e seguro. O Departamento de TI realiza o controle sobre a rede, o monitoramento dos downloads, controla o tráfego de dados das máquinas dos Colaboradores e será capaz de sugerir ou recomendar melhorias na infraestrutura tecnológica, com base no relatório emitido pelo PANDA ADPTIVE DEFENSE e ITARIAN.

O Departamento de Compliance, Controles Internos e o Comitê de Compliance visarão promover a aplicação da presente Política bem como o controle, a supervisão e a aprovação de exceções, sendo responsabilidade do Departamento de Compliance e controles internos assegurar a implementação de mecanismos eficientes capazes de resguardar a segurança das informações de propriedade do Grupo Mérito ou de terceiros em relação às quais tenha tido acesso, bem como a identificação de quaisquer infrações às regras aprovadas nesta Política.

4. Da Segurança Cibernética.

Nos termos do Código ANBIMA e da regulação em vigor, o presente Capítulo dispõe acerca da política de segurança cibernética do Grupo Mérito e tem como objetivo estabelecer as regras, procedimentos e controles de segurança cibernética que sejam compatíveis com o seu porte, perfil de risco, modelo de negócio e complexidade das atividades desenvolvidas.

Esta Política tem o objetivo de detalhar as práticas e o tratamento adequado às informações produzidas e processadas no Grupo Mérito e acordar com todos os Colaboradores os seguintes compromissos:

(i) Nossos Colaboradores mantêm reserva sobre os negócios da empresa, guardando sigilo sobre qualquer informação ainda não divulgada para o conhecimento do mercado, bem como sobre a informação de terceiros e clientes obtidos no exercício de suas funções;

(ii) Nossos Colaboradores não utilizam estas informações para obter, pessoalmente ou para terceiros, vantagens sobre qualquer natureza.

(iii) A informação é um ativo essencial para as atividades e negócios, desenvolvidos e a serem desenvolvidos pelo Grupo Mérito. Informações reservadas ou

confidenciais somente são divulgadas com autorização da Diretoria. Todo Colaborador que possui acesso a estas informações tem o cuidado de não as expor a terceiros.

O envolvimento e a adesão consciente de cada um dos Colaboradores a essa Política serão fundamentais para consolidarmos o comportamento coletivo cada vez mais atento e seguro quanto ao tratamento das informações internas.

Este documento apresenta as normas gerais para uso adequado das informações e recursos de tecnologia do Grupo Mérito e orientará nossas atitudes sobre o tema, oferecendo padrões de comportamento a serem seguidos.

4.1. Objetivo.

O objetivo desta Política visa garantir a proteção, a manutenção da privacidade, integridade, disponibilidade e confidencialidade, de forma integrada, sobre as informações de propriedade e/ou sob sua guarda do Grupo Mérito, além de prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados com o ambiente cibernético, definindo as regras que representam, em nível estratégico, os princípios fundamentais incorporados pelo Grupo Mérito para o alcance dos objetivos de segurança da informação e cibernético no desenvolvimento de suas atividades.

4.2. Aplicação.

Todas as unidades de negócios do Grupo Mérito e seus Colaboradores.

4.3. Responsabilidades.

4.3.1. Departamento de Tecnologia da Informação:

(i) Produzir relatórios e monitorar constantemente a estrutura tecnológica do Grupo Mérito para evitar, mitigar e tratar os Incidentes.

(ii) Diagnosticar, restaurar e aperfeiçoar as práticas tecnológicas e infraestrutura cibernética do Grupo Mérito

(iii) Garantir a segregação e gestão do controle de acessos, visando o cumprimento da gestão das informações.

(iv) Manter atualizada a Política de Segurança da Informação e Cibernética;

(v) Elaborar, manter atualizado e testar periodicamente um Plano de Contingência aqui descrito;

(vi) Tratar dúvidas e questões não contempladas nesta Política, a infraestrutura tecnológica do Grupo Mérito ou procedimentos de garantia cibernética do Grupo Mérito; e

(vii) Avaliar e recomendar melhorias de infraestrutura tecnológica para posterior aprovação com a Diretoria.

4.3.2. Gestores das áreas.

(i) Garantir a aplicação adequada de seus times conforme previsto nesta Política.

4.3.3. Colaboradores e demais envolvidos.

(i) Zelar pela utilização adequada das informações, e dos recursos computacionais oferecidos, em conformidade com os objetivos do negócio, missão, visão, valores e com a presente Política.

4.3.4. Departamento de Compliance e Controles internos.

(i) Realizar testes periódicos sobre a adesão dos Colaboradores frente a esta Política.

(ii) Monitorar o cumprimento e solicitar os relatórios e lastros do cumprimento desta Política ao Departamento de TI.

(iii) Avaliar e garantir a efetividade do Plano de Contingência.

(iv) Orientar os Colaboradores em situações de acionamento do Plano de Contingência.

5. Critérios e regras.

5.1. Propriedade e Proteção da Informação.

Toda a informação produzida no ambiente tecnológico do Grupo Mérito ou por ela adquirida, é considerada de sua propriedade, sendo parte do seu patrimônio, não importando a forma de apresentação ou armazenamento. Esta informação deve ser adequadamente protegida;

A informação pertencerá ao Grupo Mérito e só pode ser utilizada no seu interesse. Seu uso ou divulgação externa, por seus Colaboradores, somente poderá ocorrer quando expressamente autorizado pelo Gestor imediato ou Diretoria;

As informações devem ser utilizadas exclusivamente para fins relacionados diretamente ao negócio e desempenho da atividade do Colaborador, observando as orientações contidas nesta Política; e

O Grupo Mérito monitorará o recebimento, envio e conteúdo de todos os e-mails e documentos de sua propriedade sem prévia notificação aos Colaboradores.

6. Medidas de Segurança e Prevenção.

6.1. Classificação de informações:

Os dados serão classificados em níveis de confidencialidade, de acordo com a natureza e a criticidade das informações tratadas, restringe os níveis de acesso e reforçando os mecanismos de controle e segurança conforme a sensibilidade de cada dado. O Grupo Mérito adota as seguintes categorias para efeitos de classificação da informação:

- Publica;
- Interna;
- Confidencial;

6.2. Controle de acesso.

6.2.1. Acesso lógico, físico e sistêmico.

O Grupo Mérito, para garantir a melhor prática de segurança da informação e cibernética, realiza a segregação logica, física e sistêmica para o tráfego de informações e funcionários pelos sistemas homologados sede.

Cada usuário de recursos computacionais do Grupo Mérito deve possuir uma identificação (ID), a qual será utilizada como "conta de acesso" aos sistemas, redes e salas (físicas) da empresa conforme determinado para desenvolvimento de sua atividade e sua área;

O cadastramento do usuário para o acesso aos recursos computacionais, sistêmicos e físicos deverá ser solicitado pela Diretoria no momento da contratação, a qual estabelecerá os perfis, autorizações de acesso e logins de acesso;

A solicitação deverá ser aprovada e registrada pelo Departamento de Compliance que documentará a avaliação feita no momento de análise de Know your Employee.

O usuário deve ter acesso somente às informações e recursos que forem necessários para a realização de suas atividades e todo sistema, aplicativo possuirá, quando possível controle de logs e rastro de auditoria de modo a assegurar o uso apenas pelo usuário autorizado.

6.3. Equipamentos e Estrutura:

Os equipamentos utilizados para o desenvolvimento das atividades do Grupo Mérito são sempre atualizados conforme previsto nesta Política. Com a finalidade de garantir tal atualização o Departamento de TI incluiu como regra no sistema operacional dos computadores e o antivírus e firewalls, garantindo assim maior proteção às informações neles inseridas.

Ainda haverá a segregação da Rede Wireless para fornecedores, Clientes daquela que há ligação e acesso a rede interna do Grupo Mérito assim será garantido os requisitos de segurança, segregação e proteção dos dados definidos nesta Política.

Os equipamentos pessoais dos Colaboradores não acessam a rede Wireless corporativa, sendo vedado quaisquer outras formas de conexão de qualquer aparelho pessoal com a finalidade de conectar na rede corporativa da Grupo Mérito.

6.4. Armazenamento de Dados e Computação em Nuvem:

Os serviços de armazenamento de dados e computação em nuvem que é contratado pelo Grupo Mérito passou por uma seleção rígida que avaliou a necessidade da terceirização do serviço em questão e a confiabilidade técnica do fornecedor analisado, a fim de garantir que ele possua as qualificações de segurança necessárias. Ainda, são cumpridos todos os requisitos previstos na regulamentação específica, em especial a Resolução nº 4.893/21 do Conselho Monetário Nacional.

6.5. Obtenção de Credenciais e Gerenciamento de Acesso:

Todos os Colaboradores e prestadores de serviço essenciais assumem rígidos compromissos de confidencialidade e Compliance ao obterem as credenciais que dão acesso aos nossos dados confidenciais ou a dados classificados como sensíveis. Estas credenciais, por sua vez, são atualizadas periodicamente ou concedidas por prazo

determinado, em conformidade com as regulações e normas aplicáveis. Ainda, o acesso aos dados é restringido a menor permissão e privilégio possíveis, tendo o Departamento de TI, através do PANDA ADPTIVE DEFENSE e ITARIAN que possui a capacidade para monitorar e registrar o acesso a dados.

6.6. Avaliação de Fornecedores.

Provedores e fornecedores que armazenam e processam dados, contratados pelo Grupo Mérito são avaliados sob o ponto de vista de Segurança da Informação e Segurança Cibernética e devem seguir seus papéis e responsabilidades. O Grupo Mérito, através de seu departamento de TI, garante documentalmente que em sua análise:

- Há compatibilidade com os sistemas e controle de segurança de informação já existente e implementados;
- Possui grau de segurança de informação e cibernética, em linha com as atividade e criticidade das atividades que este fornecedor prestará ao Grupo Mérito; e
- Não haverá nenhum conflito com a infraestrutura ou garantira nenhum privilégio de acesso ou informação o fornecimento e troca com o fornecedor.

Detalhes desta seleção constam no Manual de Regras e Procedimentos para Fiscalização e Monitoramento de Prestadores de Serviço

6.7. Autenticação e Senhas

A senha é pessoal e intransferível, devendo obedecer aos padrões divulgados pela empresa. O colaborador é responsável por todas as transações realizadas nos sistemas disponibilizados;

A senha não deve, sob hipótese alguma, ser compartilhada com outras pessoas;

O usuário não deve armazenar sua senha em arquivos de computador e tampouco escrevê-la em papéis ou outro tipo de mídia; As senhas de Login na rede (WINDOWS)

aplicáveis aos aparelhos do Grupo Mérito devem estar de acordo com os seguintes aspectos:

(i) Conter no mínimo 6 (seis) caracteres;

(ii) Possuir Letras e Números; e

(iii) Devem ser criptografadas quando transmitidas ou armazenadas;

Critérios de senhas de outros sistemas de trabalho dos departamentos devem ser decididos pelos Gestores da área.

7. Rotinas, relatórios e monitoramento.

7.1. Hardware e Software

Não é permitido compra ou uso de equipamentos de Tecnologia e Softwares sem a prévia comunicação e aprovação por escrito do Departamento de TI.

Detalhes desta seleção constam no Manual de Regras e Procedimentos para Fiscalização e Monitoramento de Prestadores de Serviço

7.2. Alterações de Configuração

As configurações de hardware e software dos computadores disponibilizados pelo Grupo Mérito não poderão ser alteradas. Caso haja necessidade de algum tipo de alteração, a Diretoria deverá ser acionada através de solicitação por e-mail, com a respectiva justificativa.

Julgado necessária a alteração pela Diretoria, será enviado ao departamento de Controles Internos e Departamento TI para avaliação, aprovação e posterior implementação segura e em acordo com esta Política.

7.3. Internet

A Internet é uma ferramenta de trabalho utilizada pelos Colaboradores como apoio ao desenvolvimento de suas atividades e competências;

A autorização de acesso à Internet é monitorada pelo Departamento de Compliance e controles internos e restrita a atividades relacionadas ao desenvolvimento dos serviços do Grupo Mérito.

Não é permitido o acesso a e-mails pessoais, instalação de software de comunicação entre outros, caso necessário deverá ser solicitada autorização pelo gestor e ou Diretoria responsável; e

Utilização de *sites* não relacionada à atividade do Colaborador deverá e solicitado e aprovado pela Diretoria Responsável.

7.4. Proteção contra Software Malicioso

O software de proteção contra vírus é instalado, ativado e atualizado diariamente pelo Departamento de TI, rotina esta que é realizado em todos os computadores ligados à rede de dados do Grupo Mérito.

7.5. Cópia de Segurança (backup)

Cabe ao Departamento de TI realizar regularmente a cópia dos dados e informações mantidas nos equipamentos de armazenamento nos servidores da empresa;

Backup de e-mails armazenados é realizado, periodicamente de forma a evitar ou minimizar a perda de dados diante da ocorrência de incidentes;

Os *drives* internos e plug in externos (discos C, E, pen drives, etc.) são bloqueados para uso e não estão disponíveis para copiar, transferir armazenar dados da rede do Grupo

Mérito. A liberação será controlada pelo Departamento de TI, mediante aprovação da Diretoria.

7.6. Tratamento de Mídia

Não é permitido realizar cópia ou divulgar Informações Confidenciais existentes dentro da rede do Grupo Mérito, seja tanto para uso pessoal ou de terceiros. Tais cópias ou divulgações, quando necessárias, devem ser autorizadas pela respectiva Diretoria.

O Departamento de TI, através do PANDA ADPTIVE DEFENSE e ITARIAN, realiza o monitoramento e rastreio das transferências de dados da Rede do grupo Mérito, podendo assim atuar preventivamente e ostensivamente no bloqueio e denuncia de qualquer tentativa de obtenção sem a devida autorização.

7.7. Troca de Informações

7.7.1. Uso do Correio Eletrônico (e-mail)

O Correio Eletrônico é uma ferramenta de trabalho utilizada pelos Colaboradores como apoio ao desenvolvimento de suas atividades profissionais. Portanto, não é permitido utilizar o Correio Eletrônico para o envio de mensagens ou arquivos de conteúdo considerado impróprio pela empresa.

É considerado impróprio o conteúdo que não está em conformidade com as regras legais, a moral, a integridade e os bons costumes, tais como campanhas políticas, religiosas, venda de produtos, boatos, jogos, músicas, filmes, vídeos e fotos que não esteja na conformidade do negócio.

É proibido o download e envio de arquivos anexados ao e-mail com as extensões *.exe, *.pif, *.bat, *.com, *.scr, *.mp3, *.wav, *.wma, *.vbs, *.reg.

Todos os e-mails do domínio serão armazenados e possuem classificação de sua informação, para fins de auditorias internas e externas e poderão ser consultados com a autorização da Diretoria a qualquer momento sem prévio aviso.

7.7.2. Uso de Criptografia

O Departamento de TI, é responsável pela verificação de que toda solução de criptografia utilizada no Grupo Mérito deverá seguir as regras de Segurança da Informação e os padrões de segurança dos Órgãos reguladores.

8. Desligamentos

Na ocorrência de desligamento, independente da causa, será de responsabilidade do gestor imediato, comunicar ao Departamento de TI para realizar os bloqueios de acesso, seja de imediato ou na data do desligamento;

O Colaborador deverá entregar todos os equipamentos de sua responsabilidade para o gestor imediato, como: **CELULARES, NOTEBOOKS, PEN DRIVES E OUTROS**, sob pena de restituição de valores ou qualquer medida judicial ou extrajudicial, conforme o caso.

9. Plano de Contingência

O objetivo do Plano de Continuidade de Negócios (PCN) é apresentar um conjunto de estratégias e planos de ação que serão executados em caso de ocorrência de eventos que impeçam temporariamente a continuidade dos negócios desenvolvidos pela Mérito DTVM.

Este Plano deve prever uma resposta rápida e eficaz dada uma interrupção de negócios significativa, de modo a preservar a integridade dos colaboradores e do patrimônio do Grupo Mérito.

9.1.1. Das Contingências

O Grupo Mérito, para garantia e funcionalidade das atividades críticas que exerce vislumbra a necessidade de planejamento prévio para os seguintes grupos:

- **Contingências De Infraestruturas Físicas**: São definidas como as situações de catástrofes naturais ou não, tais como inundações, incêndios, desabamentos e etc. que impeçam o acesso e/ou utilização das instalações fiscais da sede, como também danos físicos relevantes a instalações e/ou equipamentos, intencionais ou não e ainda falhas no fornecimento de energia elétrica.
- **Contingências De Pessoal**: São definidas como os eventos que acometeriam um grupo de pessoas, acarretando o não comparecimento coletivo por motivos de greves, doença, licenças e etc.
- **Contingências De Infraestruturas Tecnológicas**: São definidas como as situações de inacessibilidade, falha ou perda de quaisquer recursos de TI, tais como hardware, software, telecom, rede e segurança.
- **Contingência De Serviços Externos**: São definidas como as situações de não prestação de serviço contratado considerado crítico / essencial aos processos e atividade do Grupo Mérito.

9.1.2. Planos de ações

9.1.2.1. Casos de contingência para infraestrutura física e tecnológica:

O prédio onde se localiza a sede das empresas do Grupo Mérito, contam com equipes de segurança 24 horas. O acesso de visitantes é dado somente com identificação por foto e documento na recepção do condomínio, mediante previa autorização da recepção do Grupo Mérito, que receberá um crachá eletrônico que permite acesso somente às catracas para os elevadores.

Assim para garantia e precaução das instalações e preservação dos controles e manutenção das atividades, será considerado o fornecimento de energia elétrica como

serviço crítico para suas atividades. Desta forma na escolha do condomínio sede foi observado e constatado a existência de geradores de energia externos, potentes o suficiente, para fornecer ao condomínio e ao Grupo Mérito a continuidade das atividades.

O Grupo Mérito, em complemento, possui dois '*nobreaks'* com capacidade de 2000va e 3000va, respectivamente, e que suportarão os sistemas de infraestrutura tecnológico, por tempo suficiente até o retorno ou acionamento de deslocamento dos funcionários conforme previso nos casos abaixo.

9.1.2.2. Casos de contingência de Pessoas.

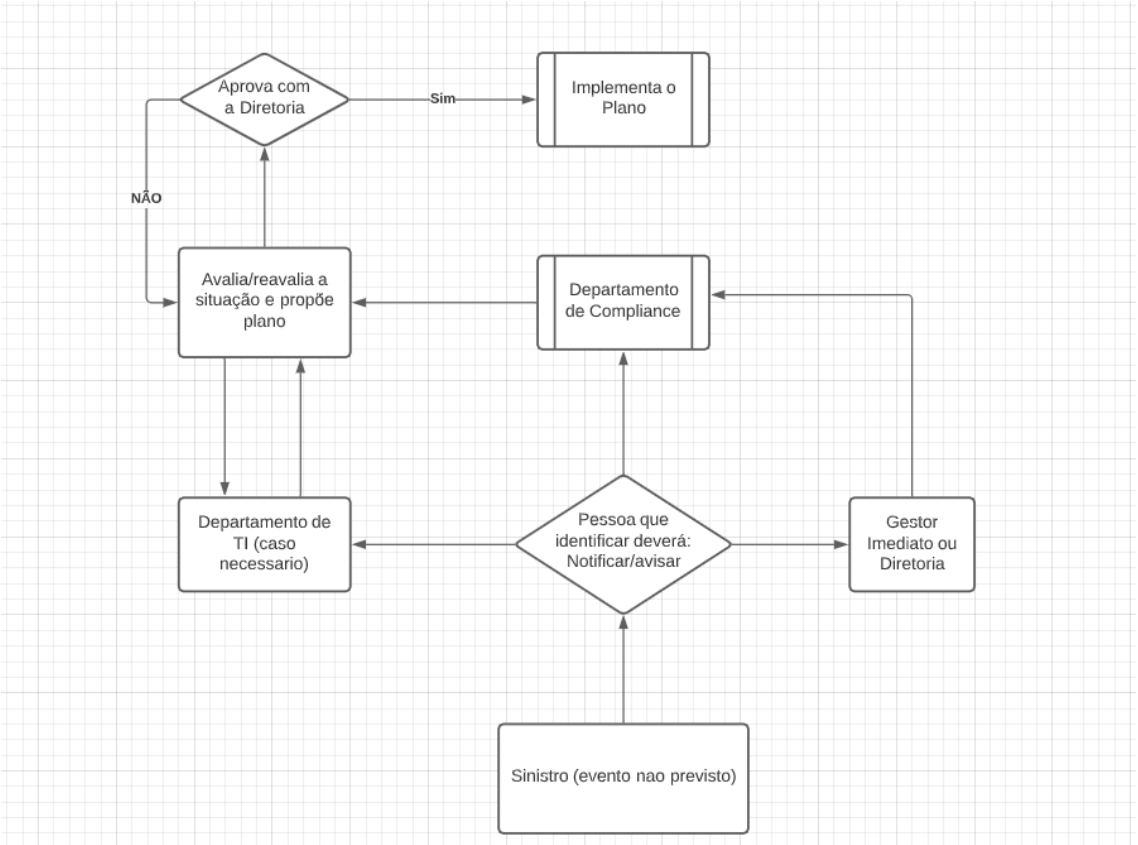
O Grupo Mérito, no exercício de suas atividades, caso depare-se com situações que inviabilizem a execução na sede ou acarretem o não comparecimento para execução de suas atividades, como primeira linha de atuação em caráter de contingencia, toda a Diretoria do Grupo Mérito possuem uma estação de trabalho completa em suas residências, com computador, impressora, acesso à internet através de fibra ótica de alta velocidade, acesso as pastas de arquivos, sistemas (respeitando a segregação funcional) e telefonia gravada, para continuidade crucial e atendimento necessário das atividades do Grupo Mérito.

9.1.2.3. Casos de contingência Serviços.

O Grupo Mérito, sempre que possível, disporá em contratos com os provedores de serviços essenciais de TI, clausulas de acordo de nível de serviço compatível para atuação em situações atípicas e essenciais para contingência.

9.1.3. Processo de contingência.

Dada a impossibilidade de previsão de todas as possibilidades para atuação e prevenção, o Grupo Mérito adotará o seguinte processo para situações ainda não previstas ou excepcionais, com fim de garantir a continuidade dos negócios:



9.1.4. Responsabilidades

9.1.4.1. Área de Tecnologia da Informação.

- Entender as necessidades sistêmicas necessárias para suportar os processos críticos e providenciar mecanismos de contingência, contemplando infraestrutura e sistemas atualmente utilizados;
- Providenciar os backups periódicos para assegurar a disponibilidade das informações;
- Atender, na medida do possível, os requisitos de Privacidade de Dados e Segurança da Informação regulados para o setor correspondente ao processo crítico;
- Efetuar os procedimentos de contingência necessário, mitigando toda a perda e ou vazamento de informações conforme prioridade definida pela Diretoria;

- Suportar as necessidades sistêmicas informadas pelos gestores nos processos críticos e no momento da crise e efetuar os procedimentos de restabelecimento do sistema principal;

9.1.4.2. Área de Complaince

- Suporte a área de Tecnologia da Informação no momento de crise auxiliando na construção do plano de contingência ideal a situação em concreto;
- Aculturamento dos colaboradores da instituição referente a correta adoção dos procedimentos de continuidade de negócios;
- Suporte a área de tecnologia da informação na execução do plano de contingência, no que for cabível.

9.1.4.3. Diretoria do Grupo Mérito.

- Aprovar os estudos e planos apresentados para a continuidade de negócios, e orientar os gestores para a correta aplicação das diretrizes assim definidas;
- Aprovar os investimentos necessários para atender os PCN;
- Declarar o momento do ingresso ao PCN, inclusive no caso de crise, bem como declarar a retomada dos procedimentos padrão;
- Aprovar os relatórios referentes aos PCN realizados pelo Departamento de TI ou compliance

9.1.4.4. Gestores ou pessoas no cargo de gestão do Grupo Mérito

- Descrever detalhadamente os procedimentos que devem ser adotados para realização dos processos críticos no momento de crise, mantendo-os devidamente as áreas impactadas atualizados destes procedimentos;
- Participar dos testes periódicos e avaliar o atingimento dos resultados esperados;

- Acionar o Departamento de Compliance através do canal de comunicação adequado;
- Respeitar as diretrizes definidas no PCN.

10. Violação da Política de Segurança da Informação

Violações a essa Política estão sujeitas a sansões disciplinares, observadas a natureza e gravidade da infração.

Caso seja identificado pelo departamento de TI ou Compliance, e ainda cada Colaborador no exercício regular de sua atividade, suspeitem de possível violação das diretrizes aqui estabelecidas todos deverão buscar a orientação nas seguintes instâncias: gestor imediato ou Departamento de TI e por fim Diretoria.

A transgressão a qualquer das regras aqui descritas e demais regras verbais ou estabelecidas pelo Grupo Mérito ou, ainda a outros códigos e políticas que o Grupo Mérito venha a aderir, será considerada infração contratual, sujeitando seu autor às penalidades cabíveis.

O Grupo Mérito não assume a responsabilidade por Colaboradores que transgridam a Lei ou cometam infrações no exercício de suas funções. Caso o Grupo Mérito venha a ser responsabilizado ou sofra qualquer prejuízo de qualquer natureza por atos de seus Colaboradores que infrinjam os princípios desta Política, será garantido o direto de exercer o direito de regresso em face dos responsáveis.

11. Treinamento e capacitação.

Os Colaboradores passarão por treinamentos periódicos referentes à prevenção e resposta à incidentes, bem como de melhores práticas de segurança cibernética, visando atingir o maior comprometimento de todos na proteção da informação e segurança cibernética. Além disso, disponibilizamos canais internos pelos quais os colaboradores possam encaminhar denúncias e suspeitas de fragilidades e violações de

segurança cibernética, a fim de agilizar assim a resposta do time especializado a eventuais incidentes.

12. Divulgação

A Grupo Mérito disponibilizará de forma publica, além desta Política de Segurança da Informação constar sempre atualizada no Portal Documentos internos do Grupo Mérito para acesso de todos os seus Colaboradores.

ANEXO I - TERMO DE ADESÃO À POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DA MÉRITO DISTRIBUIDORA DE TÍTULOS E VALORES MOBILIÁRIOS LTDA.

Atesto que recebi, li e compreendi a Política de Segurança da Informação e Cibernética ("**Política**") bem como as demais políticas e procedimentos que permeiam as atividades que desempenharei.

Ainda declaro para os devidos fins que:

Tenho total conhecimento da existência dos termos aqui previstos no qual recebi e li, sendo que me comprometo a observar integralmente seus termos e condições.

Sei, a partir desta data, que a não observância dos termos da Política do Grupo Mérito poderá implicar na caracterização de falta grave, fato que poderá ser passível da aplicação das penalidades cabíveis, inclusive demissão por justa causa.

As regras estabelecidas na presente Política do Grupo Mérito não invalidam nenhuma disposição relativa a qualquer norma interna estabelecida, mas apenas servem de complemento e esclarecem como lidar com determinadas situações na execução de minhas atividades profissionais.

Tenho ciência de que o descumprimento de qualquer regra estabelecida na Política de Sigilo e Confidencialidade, disposta na presente Política, poderá me sujeitar a penalidades e responsabilização na esfera civil e criminal. Adicionalmente, sei que, caso haja o vazamento de informação confidencial advindo da utilização de minha senha pessoal, poderei ser responsabilizado tanto civil, quanto penalmente.

Pelo presente Termo de Adesão, declaro que cumprirei todos os deveres de confidencialidade previstos na Política e nas demais políticas internas do Grupo Mérito, sob pena de responsabilização civil e criminal.

Estou ciente que o disposto na presente Política, referente as garantias de segurança da Informação e Propriedade Intelectual do Grupo Mérito, e é válido indefinidamente mesmo após o término de meu vínculo com o Grupo Mérito, não podendo ser rescindido sem expressa e inequívoca concordância junto a empresa do Grupo Mérito.

Li e entendi a legislação e regulamentação aplicável a negociação de valores mobiliários, em particular, conforme disposto na Instrução CVM nº 358/2002, conforme alterada, acerca de divulgação e o uso de informações sobre ato ou fato relevante na negociação de valores mobiliários de emissão de companhias abertas.

Reconheço e anuo expressamente a veracidade, autenticidade, integridade, validade e eficácia para assinatura deste Anexo nos termos dos artigos 104 e 107 do Código Civil, que foi por mim assinado em formato eletrônico e/ou por meio de certificados eletrônicos, inclusive os que utilizem certificados não emitidos pela ICP-Brasil, nos termos do artigo 10, § 2º da Medida Provisória nº 2.200-2, de 24 de agosto de 2001 (“MP nº 2.200-2”).”