

Classificação	
001 TEC	Políticas da Instituição Tecnologia da Informação

Título	
001	Segurança da Informação - Corporativa

Responsáveis	
Diretoria	Responsável
Diretoria Executiva Administrativo, Financeiro e TI	Thiago Herman
Gerência Geral	Responsável
Gerência Geral Administrativo, Financeiro e TI	Fabio Pestana de Abreu
Gerência	Gestor
Tecnologia da Informação	Fabio Pestana de Abreu
Autor(es)	Responsável(eis)
TI, Telecom, Suporte e Infraestrutura Controles Internos e Processos	Marcelo Silveira Lígia Couto
Contato(s) para Esclarecimentos	
TI, Telecom, Suporte e Infraestrutura Controles Internos e Processos	Marcelo Silveira Lígia Couto

Instrumento Normativo Mandatório	
<input checked="" type="checkbox"/> Política	<input type="checkbox"/> Procedimento

Impacta Matriz de Risco	
<input checked="" type="checkbox"/> Não se aplica	<input type="checkbox"/> Sim (Controle de Referência:)

Referência Legal
<ul style="list-style-type: none"> Resolução CMN 4.968 - de 25 de novembro de 2021 (revoga a Resolução 2.554/1998) Lei nº 12.846, de 01 de agosto de 2013 Resolução CVM nº 35, de 26 de maio de 2021

Documentos Vinculados
<ul style="list-style-type: none"> Princípios Éticos e Regras de Conduta Comitê de Tecnologia da Informação Política de Segurança da Informação – TI Política de Segurança Cibernética Política Programa de Home Office

Documentos Dependentes
.

Controle de Aprovação (1)	
Aprovado pela Diretoria em: 30/12/2022	Válido até: 29/12/2023

* Visando ao controle das revisões realizadas, as referidas devem ser registradas na última página do documento.

Sumário

1.	Objetivo	3
2.	Aplicação.....	3
3.	Implementação	3
4.	Regra(s) Regulamentar(es)	3
5.	Áreas Envolvidas e Responsabilidades	3
6.	Diretrizes Gerais.....	5
6.1.	Definições	5
6.2.	Princípios à Segurança da Informação	5
6.3.	Controle de Acesso	6
6.3.1.	Recursos de Tecnologia da Informação	6
6.3.2.	Segregação de Funções.....	6
6.4.	Segurança Lógica.....	6
6.4.1.	Configuração de Senhas	6
6.5.	Classificação dos Tipos de Informações Utilizadas na Instituição.....	8
6.5.1.	Informação e/ou Divulgação	8
6.6.	Recursos Humanos	9
6.6.1.	Contratação e Movimentação de Pessoas	9
6.6.2.	Ramais com Gravação de Ligações	9
6.7.	Propriedade Intelectual.....	9
6.8.	Segurança Física.....	9
6.8.1.	Áreas Seguras.....	9
6.8.2.	Acesso Físico a todas as Dependências	10
6.8.3.	Sistema de Segurança Inteligente - Biometria Digital	10
6.8.4.	Pessoas Autorizadas.....	10
6.8.5.	Autorização de Acessos	11
6.9.	Uso dos Recursos de Tecnologia da Informação	11
6.9.1.	Uso da <i>Internet</i>	11
6.9.2.	Uso de <i>E-mail</i>	12
6.9.3.	Instalação de <i>Softwares</i> ou Aplicativos.....	12
6.9.4.	Uso das Redes Sociais	12
6.9.5.	Descarte de Informações.....	12
6.10.	Processo – Mesa Limpa e Tela Limpa.....	13
6.11.	Regras Específicas Sobre Segurança da Informação – TI, Segurança Cibernética e Programa <i>Home Office</i>	13
6.12.	Sigilo, Segurança da Informação, Privacidade e Proteção de Dados	13
7.	Conformidade.....	14
7.1.	Lei Anticorrupção e Confidencialidade das Informações	14
8.	Exceção às Regras estabelecidas Neste Instrumento Normativo	14
9.	Versionamento	15

1. Objetivo

Estabelecer as regras e diretrizes de segurança da informação, visando no mínimo, proteger as informações e ativos da RENASCENÇA DTVM LTDA. (“Renascença”) e dos clientes em geral, bem como reduzir o risco de ocorrência de acessos indevidos ou modificações não autorizadas, em conformidade com o determinado pela Diretoria Executiva, pelas normas e legislação vigentes.

2. Aplicação

As regras estabelecidas neste documento devem ser cumpridas pelos dirigentes, funcionários e prestadores de serviços (“Colaboradores” / “Colaborador”) vinculados à Renascença.

3. Implementação

Imediata, a partir da publicação na *Intranet* Corporativa – Instruções Normativas. Esta Política substitui documento POL 20 – Segurança da Informação - Corporativa.

4. Regra(s) Regulamentar(es)

- [Resolução CMN Nº 4.968, de 25 de novembro de 2021](#): Dispõe sobre os sistemas de controles internos das instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil.
- [Lei nº 12.846, de 01 de agosto de 2013 - Lei Anticorrupção](#): Dispõe sobre a responsabilização administrativa e civil de pessoas jurídicas pela prática de atos contra a administração pública, nacional ou estrangeira, e dá outras providências.
- [Resolução CVM nº 35, de 26 de maio de 2021](#): Estabelece normas e procedimentos a serem observados na intermediação de operações realizadas com valores mobiliários em mercados regulamentados de valores mobiliários e revoga a Deliberação CVM nº 105, de 22 de janeiro de 1991, e as Instruções CVM nº 51, de 9 de junho de 1986, CVM nº 333, de 6 de abril de 2000, CVM nº 505, de 27 de setembro de 2011, Instrução CVM nº 526, de 21 de setembro de 2012; Instrução CVM nº 581, de 29 de setembro de 2016; Instrução CVM nº 612, de 21 de agosto de 2019; e Instrução CVM nº 618, de 28 de janeiro de 2020.

5. Áreas Envolvidas e Responsabilidades

Diretoria Executiva Administrativo, Financeiro e TI

- Aprovar a Política de Segurança da Informação - Corporativa, em consonância com as regulamentações vigentes e diretrizes definidas pela Diretoria Executiva;
- Participar do processo deliberativo (como 2ª instância – onde ocorre a deliberação do risco a ser assumido pela Instituição) relacionado às solicitações de acessos Tipo E – Exceção;
- Estabelecer decisões administrativas referentes aos casos de descumprimento desta Política.

Gerência Geral Administrativo, Financeiro e TI Gerência de Tecnologia da Informação

- Aprovar as regras estabelecidas nesta Política juntamente com o Diretor Executivo Administrativo, Financeiro e TI;
- Assegurar a efetividade e continuidade da aplicação desta Política;
- Garantir que medidas corretivas sejam adotadas quando falhas de conformidade forem identificadas;
- Assegurar, juntamente com a Área de *Compliance*, que a Política esteja em conformidade com as regulamentações vigentes e determinação da Diretoria Executiva;
- Emitir parecer acerca das ações a serem implementadas para correção das deficiências apontadas;
- Orientar as áreas e gestores a respeito dos procedimentos e práticas a serem cumpridas;
- Responder aos requerimentos dos Órgãos Reguladores.

Área de Recursos Humanos

- Informar de maneira imediata as áreas envolvidas sobre contratação, desligamento, afastamento e modificações no quadro visando garantir a execução dos procedimentos necessários.

Compliance

- Promover a disseminação desta Política, bem como aculturar os Colaboradores acerca das regras pertinentes;
- Garantir que as regras estabelecidas nesta Política estejam de acordo com o determinado pela Diretoria Executiva e regulamentações vigentes;
- Avaliar em conjunto com as Áreas de Controles Internos e Processos e TI – Telecom, Suporte e Infraestrutura os riscos relacionados à segurança da informação e apresentar propostas de aperfeiçoamento do ambiente de controle, quando for o caso.
- Fazer com que todos os colaboradores, prestadores de serviços de TI e terceiros contratados de TI tenham conhecimento deste documento;
- Manter esta Política devidamente atualizada, juntamente com as Áreas de Controles Internos e Processos e TI – Telecom, Suporte e Infraestrutura;
- Participar do processo deliberativo (como 1ª instância) relacionado às solicitações de acessos Tipo E - Exceção.
- Caso sejam constatadas quaisquer atipicidades, conduzir investigações internas e sigilosas, verificando se há indícios de irregularidades, de modo a combatê-las com base nas boas práticas e determinações de governança.

Controles Internos e Processos

- Coordenar o desenvolvimento de mecanismos para o controle e a mitigação dos riscos, visando ao subsídio de planos de ação para a correção de falhas operacionais, especialmente àquelas as quais possam impactar as atividades da Renascença como um todo;
- Monitorar a aderência à Política e avaliar, periodicamente, a efetividade desta, identificando e corrigindo eventuais deficiências;
- Garantir, em conjunto com a Área de TI – Telecom, Suporte e Infraestrutura, os processos para prover a continuidade de negócios.
- Desenvolver e implementar controles, visando garantir que regras informadas neste documento, estejam sendo executadas com qualidade por todos colaboradores, prestadores de serviços de TI e terceiros contratados de TI da Renascença DTVM;
- Manter esta Política devidamente atualizada, juntamente com as Áreas de *Compliance* e TI – Telecom, Suporte e Infraestrutura.

Colaboradores e Terceiros Prestadores de Serviços Vinculados à Renascença

- Informar à gestão imediata e à Área de TI – Telecom, Suporte e Infraestrutura, por *e-mail* ou outro meio de comunicação eficiente, qualquer ação que não condiz com o determinado nesta Política;

- Cumprir integralmente as regras determinadas nesta Política.

Área de TI – Telecom, Suporte e Infraestrutura

- Desenvolver e manter procedimentos e ações que visam garantir a disponibilização da informação de forma íntegra e segura;
- Adotar postura crítica quanto aos riscos envolvidos, evidenciada por meio de ambientes de controle, com o objetivo de propor planos de ação para a melhoria dos processos, visando à mitigação de possíveis impactos à Renascença;
- Assegurar, juntamente com a Área de *Compliance*, que a Política esteja em conformidade com as regulamentações vigentes e determinação da Diretoria Executiva;
- Manter esta Política devidamente atualizada, juntamente com as Áreas de *Compliance* e Controles Internos e Processos.

Auditoria Interna

- Auditar e testar periodicamente os mecanismos para acompanhamento, controle e mitigação dos possíveis riscos pertinentes à Segurança da Informação, inclusive assegurando a verificação de sua eficácia e efetividade; e
- Avaliar os sistemas (fontes de informação, integridade e completude dos dados), bem como a adequação e conformidade dos processos.

6. Diretrizes Gerais

6.1. Definições

- **Conceito de Informação:** A informação é um elemento essencial para todos os processos de negócios da Renascença, portanto, considerada como bem ou ativo de grande valor. Portanto, deve estar adequadamente protegida em todo o seu ciclo de vida, que compreende, geração, manuseio, armazenamento, transporte e descarte.
- **Segurança da Informação:** Consiste na proteção da informação de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio.

6.2. Princípios à Segurança da Informação

A Renascença utiliza elevados padrões tecnológicos de segurança de rede para evitar fraudes, invasões e garantir o sigilo de todas as informações e comunicações interna e externa. A segurança da informação é caracterizada pela preservação de três aspectos básicos:

1. **Confidencialidade:** Garante que a informação seja acessível somente pelas pessoas autorizadas, pelo período necessário.
2. **Integridade:** Garante que a informação esteja completa e íntegra e não modificada ou destruída de maneira não autorizada ou acidental durante o seu ciclo de vida.
3. **Disponibilidade:** Garante que a informação esteja disponível para as pessoas autorizadas, sempre que necessário.

6.3. Controle de Acesso

6.3.1. Recursos de Tecnologia da Informação

Os acessos aos Recursos de TI devem ser concedidos, somente, após o cadastramento dos devidos direitos do colaborador, prestador de serviços de TI ou terceiro contratado de TI no

Sistema ADROIT – SAS, devendo ser consideradas as atividades com a qual a função esteja relacionada.

As permissões de acesso (determinadas na Matriz de Segregação de Funções) devem ser revisadas anualmente, de forma que seja evitado acesso não previsto ou incompatível com Matriz, bem como o conflito de interesse, pela Área de TI juntamente com os gestores responsáveis e com os Proprietários de Informação. Esse processo deve ser realizado para corroborar na elaboração do [Relatório Anual de Controles Internos](#).

Devido ao processo de revisão anual, a Matriz de Segregação de Funções deve ser datada no momento da publicação, bem como devem ser arquivadas as versões anteriores, visando a preservação da informação e disponibilização de evidências, caso sejam necessárias. É importante ressaltar que, havendo necessidade, a Matriz de Segregação de Funções pode ser revisada a qualquer momento, visando o atendimento à regulamentação e à Instituição.

Toda violação de acesso identificada deve ser comunicada, via e-mail, à Diretoria de TI e à Área de *Compliance* e Controles Internos, para análise e providências.

6.3.2. Segregação de Funções

Sendo um dos princípios basilares de Controle Interno da Administração, a Segregação de Funções consiste na separação de atribuições ou responsabilidades entre diferentes colaboradores, especialmente as funções de comercialização, aprovação de operações, controle, contabilização, auditoria e consulta devem ser apartadas.

Todos colaboradores não devem, em hipótese alguma, possuir poderes e/ou atribuições em desacordo com essa determinação.

O controle efetivo junto a Matriz de Segregação de Funções deve ser mantido de maneira consistente, visando o acesso seguro e rápido aos Colaboradores, , garantindo de forma confiável a restrição de acessos indevidos e/ou maliciosos. O detalhamento deste processo está descrito no [Manual de Controles Internos - Concessão de Acessos aos Sistemas - Segregação de Funções](#), onde constam os seguintes fluxos de solicitação e aprovação:

- Inclusão de novos Colaboradores ou Terceiro Contratado de TI ou Prestador de Serviços de TI;
- Manutenção - Alteração de Área (processo de transferência entre áreas);
- Manutenção - Alteração de Acesso (mantendo-se na mesma área);
- Desligamento ou Rescisão de Contrato de Prestação de Serviços;
- Acesso Tipo E – Exceção.

Fica declarado que, os fluxos de solicitação e aprovação devem ser realizados impreterivelmente pelos responsáveis determinados na Matriz de Segregação de Funções.

6.4. Segurança Lógica

6.4.1. Configuração de Senhas

Os Colaboradores- são responsáveis pela confidencialidade de suas respectivas senhas, lembrando que as mesmas são individuais e intrasferíveis.

Devem ser seguidas as regras determinadas pela Área de Tecnologia da Informação – Segurança da Informação, no momento da configuração e do cadastramento de senha, sendo:

SENHAS DE ACESSO AOS SISTEMAS

(Requisitos mínimos em conformidade com o definido pelo Órgão Regulador)

- Tamanho mínimo	- 06 (seis) caracteres
- Tempo máximo de expiração	- 90 (noventa) dias
- Quantidade máxima de tentativas antes do bloqueio	- 05 (cinco)
- Duração do bloqueio	- Desbloqueio mediante avaliação do administrador
- Histórico mínimo de senhas utilizadas	- 06 (seis)
- Complexidade ativada	- Letras maiúsculas, letras minúsculas, caracteres e números
- Forma de armazenamento	- Por criptografia

SENHAS DE ACESSO À REDE CORPORATIVA

(Requisitos mínimos em conformidade com o definido pelo Órgão Regulador, **com acréscimo de complexidade**)

- Tamanho mínimo	- 07 (sete) caracteres
- Tempo máximo de expiração	- 30 (trinta) dias
- Quantidade máxima de tentativas antes do bloqueio	- 03 (três)
- Duração do bloqueio	- Desbloqueio mediante avaliação do administrador
- Histórico mínimo de senhas utilizadas	- 24 (vinte e quatro)

- Complexidade ativada	- Letras maiúsculas, letras minúsculas, caracteres e números
- Forma de armazenamento	- Por criptografia

SENHAS DE ACESSO DOS CLIENTES – FERRAMENTAS DE NEGOCIAÇÃO DMA E SISTEMAS INTERNOS

- Tamanho mínimo	- 06 (seis) caracteres
- Quantidade máxima de tentativas antes do bloqueio	- 05 (cinco)
- Senha bloqueada	- Somente deve ser desbloqueada mediante confirmação da identidade do usuário (confirmação de dados pessoais, cadastrais e/ou operações) pela Renascença
- Manutenção e forma de armazenamento	- Por criptografia
- A senha deve ser trocada ao primeiro acesso	

6.5. Classificação dos Tipos de Informações Utilizadas na Instituição

Dada a sua importância, a informação deve ser classificada de acordo com o grau de confidencialidade, relevância e criticidade para os negócios da Renascença e ficar evidente e de fácil conhecimento pelos Colaboradores.

6.5.1. Informação e/ou Divulgação

Estratégica

Informação e/ou divulgação muito sensível e exclusiva para uso interno. A divulgação não autorizada pode causar impactos negativos ou prejuízos à Instituição.

Restrita

Tipo de informação e/ou divulgação que pode paralisar a operação, acarretar prejuízos pela sua divulgação indevida, podendo gerar penalidades previstas em leis e outras consequências graves à Instituição.

Interna

Informação e/ou divulgação que possui acesso irrestrito aos colaboradores, prestadores de serviços de TI ou terceiros contratados de TI. A divulgação para o público externo deve ser, impreterivelmente, autorizada pelo Gestor responsável pelo conteúdo.

Pública

Informação aberta ao público externo. É importante ressaltar que essa definição não se enquadra, sob hipótese alguma, às informações relacionadas aos processos operacionais.

6.6. Recursos Humanos

6.6.1. Contratação e Movimentação de Pessoas

Informação e/ou divulgação muito sensível e exclusiva para uso interno. A divulgação não autorizada pode causar impactos negativos ou prejuízos à Instituição.

Todos Colaboradores contratados - devem tomar conhecimento desta política e cumprir todas as regras descritas, o mesmo tratamento deve ser dado ao [Código de Ética e Conduta](#) e o [Termo de Responsabilidade](#) para acesso à Rede Renascença, assumindo o dever sobre sigilo, mesmo quando desligado, das informações relacionadas aos sistemas, processos e operações.

O Termo de Responsabilidade deve ser assinado pelos Colaboradores e deve ser revisto sempre que ocorrer alteração no contrato (de prestadores de serviços de TI ou de terceiros contratados de TI), bem como no processo de desligamento do colaborador.

6.6.2. Ramais com Gravação de Ligações

Os colaboradores de áreas com exigência regulatória de gravação de ramais, devem estar cientes que todas as conversas realizadas são gravadas. A gravação deve ser arquivada em formato digital pelo prazo mínimo de 05 (cinco) anos. Para mais informações sobre o tema, verificar a [Política Gravação de Voz \(POL 23\)](#).

6.7. Propriedade Intelectual

O colaborador deve ter ciência que, os direitos de autoria e propriedade intelectual relativos aos programas de computador, sistemas e demais suportes tecnológicos a que vier ter acesso e/ou desenvolver durante a vigência de seu vínculo profissional, pertencem exclusivamente à Instituição.

Ficando certo que, a compensação relacionada ao trabalho do colaborador, associada à pesquisa e ao desenvolvimento, está vinculada somente à remuneração contratual acertada.

6.8. Segurança Física

6.8.1. Áreas Seguras

Deve ser considerada como Área de Segurança toda instalação que possui servidores de aplicação, bancos de dados, *firewall*, unidade de *backup* e a Mesa de Operações. Não é permitida a presença de Clientes, em qualquer hipótese, no ambiente da Mesa de Operações.

As dependências da Sala dos Servidores devem respeitar os seguintes requisitos:

- Possuir piso elevado para melhor distribuição e estrutura de cabeamento;
- Não possuir meios alternativos de acesso como janelas ou portas secundárias;
- Possuir alimentação de energia independente e em conformidade com as especificações dos fabricantes dos equipamentos instalados;
- Possuir extintor;
- Ar condicionado;
- Sensor de temperatura e umidade, para manter a eficiência operacional;
- Termômetro, para controlar e monitorar o ambiente da sala.

6.8.2. Acesso Físico a todas as Dependências

O acesso físico às Áreas Seguras deve ser restrito às pessoas autorizadas.

Os acessos devem ficar registrados para fins de monitoramento e auditoria por um período não inferior à 05 (cinco) anos.

Terceiros que necessitam ter acesso a Sala dos Servidores devem ser submetidos a todas as normas de segurança descritas nesta Política, sendo que o acesso e o serviço devem ser acompanhados por pessoa qualificada e autorizada.

Todo Colaborador deve possuir uma credencial (crachá), para acesso à entrada principal do prédio e elevadores.

O acesso de prestadores de serviços de TI ou terceiros contratados de TI e não contratados de TI, à Instituição, deve ser monitorado, para tanto, as regras a seguir devem ser cumpridas:

- A credencial (crachá) é pessoal e intrasferível, portanto, não é permitido o uso por outros prestadores de serviços de TI ou terceiros contratados de TI.
- A responsabilidade pela conservação e integridade da credencial é de cada prestador de serviço ou terceiro, no caso de perda ou extravio, a área responsável pela contratação deve ser informada imediatamente para o bloqueio da mesma e demais providências cabíveis.

6.8.3. Sistema de Segurança Inteligente - Biometria Digital

A Instituição possui sistema de segurança inteligente, controlado através de sistema de biometria digital, para o ingresso em suas dependências. Estão instalados 05 (cinco) leitores de biometria digital, para controle de acesso físico, distribuídos da seguinte maneira:

- Recepção - Registro de controle de acesso de entrada principal na Renascença;
- Recepção - Registro de controle de acesso de saída;
- CPD - Registro de controle de acesso de entrada;
- Sala Operações Porta 1 - Registro de controle de acesso de entrada;
- Sala Operações Porta 2 - Registro de controle de acesso de entrada.

Através deste sistema fica restrito o acesso de pessoas não autorizadas.

6.8.4. Pessoas Autorizadas

As autorizações para configurar as permissões de acesso foram estipuladas pela Diretoria Executiva Administrativo, Financeiro e TI, em conformidade com as regras e parâmetros internos; e Roteiro Básico do Programa de Qualificação Operacional (PQO) que compreende uma série de requisitos e práticas operacionais, baseadas nas regras do Banco Central, da Comissão de Valores Mobiliários (CVM) e das próprias normas de autorregulação da B3.

As pessoas autorizadas para o acesso físico às dependências da Renascença:

Diretores

- Os Diretores possuem acesso irrestrito.

Operadores de Mesa de Títulos Privados, Mesa de Títulos Públicos, Mesa de Operações Derivativos, Mesa de Operações Segmento *Equities*, *Middle Office* Privados, *Middle Office* Derivativos, *Middle Office* Renda Fixa e *Compliance*

- Acesso à Sala de Operações, respeitados os dias e horários permitidos.

Analistas de TI, *Telecom*, Suporte e Infraestrutura

- Acesso ao CPD, respeitados os dias e horários permitidos.
- Acesso à Sala de Operações, para atendimento a chamado técnico local.

Colaboradores

- Todos os colaboradores devidamente cadastrados no sistema de acesso terão direito de entrar nas dependências físicas da Renascença, respeitados os horários e dias permitidos, ao passo que para cada colaborador será informado, por escrito, quanto às suas permissões. O colaborador poderá solicitar alterações, que serão devidamente autorizadas, quando e conforme seja necessário.

Visitantes

- São atendidos pela recepcionista e só poderão entrar nas dependências internas mediante o acompanhamento de pessoa autorizada da Renascença. Por sua vez, é efetuado um registro da identidade do visitante na portaria do prédio e, em seguida, a recepção da Renascença controla a liberação de acesso à Instituição.

6.8.5. Autorização de Acessos

Os Analistas de TI, *Telecom*, Suporte e Infraestrutura podem conceder acesso, conforme descrito no **Item Pessoas Autorizadas**. As solicitações de qualquer alteração, em virtude de trabalho extra ou fora de horário, ou por qualquer outra razão, devem ser encaminhadas por e-mail para rh@dtvm.com.br e a Área de Recursos Humanos deve pedir autorização do Diretor responsável para proceder com a alteração. Nenhuma alteração deve ser realizada sem a devida autorização formal dos responsáveis citados.

6.9. Uso dos Recursos de Tecnologia da Informação

Todos Colaboradores que tiverem acesso a ativos da informação são responsáveis pela sua integridade e confidencialidade.

6.9.1. Uso da *Internet*

A Instituição disponibiliza acesso à *internet* aos seus Colaboradores, com o objetivo de proporcionar recursos complementares, quando necessário, na realização de suas atribuições, mas em hipótese alguma a Instituição permite a execução de *softwares* da *internet*.

Havendo a necessidade de efetuar *downloads* ou de acessar um endereço na *internet* que esteja bloqueado pelas ferramentas de controle, o gestor responsável deve encaminhar, por e-mail, uma solicitação com os devidos detalhes à Área de TI para a análise e, se possível, deliberação.

A Instituição não aprova, em hipótese alguma, o uso indevido ou de maneira ofensiva da *internet*, ficando os colaboradores, prestadores de serviços de TI ou terceiros contratados de TI sujeitos à advertência e/ou às penalidades administrativas cabíveis.

Não são permitidos, em hipótese alguma, a divulgação e/ou o compartilhamento indevido de informações relacionadas à Instituição em *sites*, comunidades de relacionamento, salas de bate-papo, *chat* ou qualquer outra forma de comunicação que venha a ser desenvolvida e utilizada por meio da *Internet*.

6.9.2. Uso de E-mail

Os usuários desse recurso, ou seja, emitentes (entre eles, colaboradores, prestadores de serviços de TI ou terceiros contratados de TI) da Renascença DTVM devem veicular, por meio de *e-mail*, as informações descritas como propriedade da Instituição, e não como particular junto ao destinatário.

Com o intuito de preservar a segurança da informação veiculada, a Instituição reserva-se o direito de monitorar o conteúdo de todas as mensagens recebidas ou geradas via este recurso tecnológico.

6.9.3. Instalação de Softwares ou Aplicativos

A Instituição não aprova a instalação de qualquer tipo de *software* ou aplicativo, sem a devida deliberação realizada pela Área de TI. O não cumprimento dessa diretriz pode promover problemas relacionados aos códigos maliciosos e/ou contaminação do ambiente tecnológico, caso o mesmo ocorra, o colaborador responsável deve responder por suas respectivas ações.

6.9.4. Uso das Redes Sociais

Comentários relacionados aos processos e as atividades executadas na Instituição, não devem ser realizados (por áudio, texto ou vídeos) nos meios de comunicação social, mesmo que já tenham se tornado público por meio da mídia.

Os Colaboradores devem assegurar a confidencialidade e a integridade das informações pertencentes à Instituição.

6.9.5. Descarte de Informações

Todos os Colaboradores devem proteger as informações que lhes foram confiadas, principalmente aquelas com potencial para gerar vantagens competitivas ou capazes de gerar impactos financeiros, de imagem ou jurídicos.

Todos os documentos que possuem informações sensíveis, devem ser descartados por meio de fragmentadoras, sendo eles:

- Códigos de programas;
- Qualquer tipo de contrato;
- Relatórios restritos;
- Documentos que contenha informações de clientes, entre eles, extratos, relatórios e propostas.

O descarte de mídias deve ser realizado conforme segue:

- Cartões de crédito ou banco: cortados em pequenos pedaços, devendo a área magnética ser invalidada;-
- CDs, DVDs e *pendrives*: quebrados em alguns pedaços;
- Discos rígidos devem ser formatados fisicamente e devem ser destruídos de forma a evitar sua reutilização.

6.10. Processo – Mesa Limpa e Tela Limpa

Os processos mesa limpa e tela limpa asseguram que as informações sensíveis, tanto em formato digital quanto físico, e ativos (*notebooks*, celulares, *tablets*, etc.) não sejam deixados desprotegidos em espaços de trabalho pessoais ou públicos quando não estão em uso, ou quando alguém deixa sua área de trabalho, seja por um curto período de tempo ou ao final do dia. Seguem demais ações que auxiliam neste processo:

- Computadores pessoais e terminais de computador não devem ser deixados logados, caso o responsável não esteja presente.
- Destruir os documentos impressos antes de jogá-los. Sempre que possível utilizar máquinas fragmentadoras. Caso não haja informações confidenciais, utilizar o verso ou as partes em branco da folha como rascunho.

Essas ações visam a sustentabilidade e a redução do risco de violação de segurança, fraudes e roubos de informações.

6.11. Regras Específicas Sobre Segurança da Informação – TI, Segurança Cibernética e Programa *Home Office*

A Renascença, entendendo a importância da segurança da informação, possui regras específicas para que visam proteger os ativos de tecnologia e os dados dos seus clientes. Deste modo, toda atividade desempenhada na Instituição, bem como a ela relacionada, deverá respeitar os princípios estabelecidos nas Políticas informadas a seguir:

- Regras referentes à proteção lógica da informação da Instituição e relacionadas especificamente à Área de TI estão estabelecidas na [Política de Segurança da Informação – TI](#).
- Regras pertencentes à Segurança Cibernética, acessos às informações sensíveis de clientes e parceiros, estão determinadas na [Política de Segurança Cibernética](#). A Instituição entende que a segurança cibernética se refere a um conjunto de práticas que protege a informação armazenada nos computadores e aparelhos de computação, sendo transmitida por meio das redes de comunicação, incluindo a *internet* e telefones celulares.
- Regras e as diretrizes associadas à proteção das informações, bem como à execução das atividades laborativas em domicílio, com observância aos princípios de ética, responsabilidade e diligência estão estabelecidas na [Política Programa Home Office](#).
- Regras e ações relacionadas às melhorias e alterações com base nos riscos potenciais conhecidos e demais assuntos de Tecnologia da Informação e Segurança da Informação estão determinadas no [Comitê de Tecnologia da Informação](#).

6.12. Sigilo, Segurança da Informação, Privacidade e Proteção de Dados

A Renascença observa e cumpre toda a legislação aplicável à segurança da informação, privacidade e proteção de dados, inclusive (sempre e quando aplicáveis) à Constituição Federal, ao Código de Defesa do Consumidor, Código Civil, Marco Civil da Internet (Lei Federal nº 12.965/2014) e seu decreto regulamentador (Decreto 8.771/2016), à Lei Complementar nº 105/2001 (Lei do Sigilo Bancário), à Lei Complementar nº 166/2019 (altera a LC 105/2001), à Lei Federal nº 13.709/2018 (Lei Geral de Proteção de Dados - “LGPD”), à Lei nº 13.853/2019 (altera a LGPD) e demais normas setoriais ou gerais sobre o tema. Para tanto, adota as medidas necessárias para garantir a confiabilidade de qualquer colaborador a ela vinculado, que venha a ter acesso aos dados pessoais coletados e tratados no âmbito do relacionamento com clientes, garantindo que o acesso esteja estritamente limitado àqueles

que de fato precisam fazê-lo, de forma sigilosa e confidencial e em observância às disposições da LGPD e demais normas aplicáveis ao tema.

Em caso de armazenamento de dados pessoais e/ou dados sensíveis relacionados aos clientes, a Renascença respeitará os padrões adequados de segurança, sigilo e confidencialidade, ficando o referido processo sujeito às auditorias regulatórias.

A LGPD conceitua “dados pessoais” e “dados sensíveis”, ficando tais conceitos definidos como sendo (i) “dados pessoais”: informações relacionadas à pessoa natural identificada ou identificável; e (ii) “dados sensíveis”: dado pessoal passível de discriminação, tais como: 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 vinculado a uma pessoa natural.

No âmbito do relacionamento com os clientes, a Renascença estabelecerá controles de governança técnicos e administrativos internos que garantam a integridade e disponibilidade dos dados pessoais tratados, além de garantir a conformidade com a LGPD e demais normas aplicáveis ao tema.

7. Conformidade

7.1. Lei Anticorrupção e Confidencialidade das Informações

A Renascença pauta suas atividades agindo com integridade e honestidade em suas práticas gerenciais e em suas operações comerciais, combatendo a corrupção e o suborno em todas as suas formas, especialmente por meio de seus colaboradores, fornecedores, terceiros e administradores. Desta forma, é vital para a Instituição que todos os mencionados tenham conhecimento e observem todas as normas relacionadas à anticorrupção e suborno, sobretudo a Lei nº 12.846 de 01/08/2013 (“Lei Anticorrupção”).

Informações relacionadas às negociações e aos sistemas da Renascença deverão ser mantidas de forma confidencial, inclusive em virtude da possibilidade de acesso remoto dos Colaboradores às referidas informações. Portanto, todo cuidado deve ser tomado quanto ao que é dito, escrito ou comunicado, inclusive, eletronicamente, mesmo que em ambiente de trabalho remoto.

Neste íterim, todos os Colaboradores deverão proteger as informações relacionadas às atividades da Instituição, devendo empregar o máximo dever de sigilo quanto aos dados obtidos em virtude, inclusive, mas não se limitando, aos acessos remotos efetuados dentro do Programa *Home Office*.

Com vistas à manutenção de sua reputação, ao cumprimento da Lei Anticorrupção e à confidencialidade das informações, a Renascença instituiu o [Instrumento Normativo Princípios Éticos e Regras de Conduta](#), cujo conteúdo deve ser amplamente divulgado e observado.

8. Exceção às Regras estabelecidas Neste Instrumento Normativo

Em havendo qualquer exceção relacionada às regras e diretrizes estabelecidas nesta Política, esta deverá ser aprovada, em primeira instância, pela Diretoria Executiva Administrativo, Financeiro e TI e pela Gerência Geral Administrativo, *Compliance* e Ouvidoria.

9. Versionamento

Versão:	Data de Revisão:	Histórico:
1	12/2019	Versão anterior, o histórico do conteúdo e as aprovações, estão arquivados sob a responsabilidade da Área de Compliance.
2	30/12/2020	Revisão total do conteúdo e inserção do novo modelo de normativo adotado pela Instituição. Esta Política substitui o documento POL 20 – Segurança da Informação – Corporativa.
3	30/12/2021	Revisão total do conteúdo.
4	30/12/2022	Revisão anual do conteúdo.