REAL GRANDEZA
Fundação de Previdência e Assistência Social

DA

POLÍTICA
SEGURANÇA E TECNOLOGIA DA INFORMAÇÃO

Versão: 4

2022

REAL GRANDEZA
Fundação de Previdência e Assistência Social

DA

POLÍTICA
SEGURANÇA E TECNOLOGIA DA INFORMAÇÃO

Versão: 4

Aprovado em: 28 / 06 / 2022

Documento de Aprovação: RC Nº 001 / 534

SUMÁRIO

ASSUNTO	PÁGINA

1. INTRODUÇÃO

1. A Política de Segurança e Tecnologia da Informação - PSI registra os objetivos, princípios e as diretrizes de Segurança da Informação adotadas pela REAL GRANDEZA, que devem ser observados por todos os membros dos órgãos estatutários, dos comitês, dos Grupos de Trabalho, Comissão de Ética, empregados, estagiários, jovens aprendizes, participantes, assistidos, patrocinadoras, instituidores, fornecedores de produtos e serviços, prestadores de serviços de saúde, autoridades e outras partes interessadas, devendo ser aplicada nos recursos administrativos e tecnológicos, de caráter permanente ou temporário, pertencentes às áreas de negócio da REAL GRANDEZA.

2. OBJETIVO

O objetivo da presente Política é propiciar a busca pelas melhores práticas de Segurança da Informação e a melhoria dos serviços prestados para atendimento às necessidades e expectativas dos negócios da REAL GRANDEZA, por meio do estabelecimento, implantação, operação, análise crítica, monitoramento, manutenção e melhoria contínua de um Sistema de Gestão de Segurança da Informação, bem como por meio de adoção de princípios, regras e práticas de governança, gestão e controle adequados ao porte, complexidade e riscos inerentes aos planos que opera, destacando-se:

2.1. Promover a informatização dos processos, estimulando a ampla utilização da Tecnologia da Informação - TI para apoio à gestão e suporte das suas atividades;

2.2. Promover a convergência e integração de redes, serviços e sistemas de informação;

2.3. Maximizar o retorno dos investimentos em TI, com a implantação de projetos eficientes, otimizando a aplicação dos recursos financeiros disponíveis;

2.4. Disseminar as melhores práticas na gestão e na manutenção da infraestrutura de TI, inclusive por meio da ampla divulgação do Código de Conduta e Ética da REAL GRANDEZA;

2.5. Incentivar a utilização de portal corporativo, por meio da Internet e Realnet, como ferramenta de comunicação com as partes interessadas;

2.6. Estimular a utilização de documentação digital, empregando conceitos e técnicas de gestão eletrônica de documentos;

2.7. Padronizar tecnologias, visando a interconexão, integração e intercâmbio de aplicações entre as áreas de negócio, além da redução de custos;

3. PRINCÍPIOS

3.1. Visando garantir a Segurança da Informação na REAL GRANDEZA, por meio do estabelecimento de diretrizes para criação, transmissão, processamento, utilização, armazenamento, recuperação e descarte de informações, devem ser observados os seguintes princípios:

3.1.1. Integridade: Garantir que a informação seja mantida em seu estado original, exata e completa.

3.1.2. Confidencialidade: Garantir que o acesso à informação esteja disponível somente para pessoas, entidades ou processos autorizados.

3.1.3. Disponibilidade: Garantir que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

4. DIRETRIZES

4.1. As ações e projetos de TI devem sempre considerar o retorno do investimento, buscar a otimização na aplicação dos recursos, a redução de gastos gerais com TI, o compartilhamento de recursos e a troca de experiências entre as diversas áreas de negócios.

4.2. Os riscos devem ser continuamente identificados, analisados, avaliados, tratados e reduzidos a um nível aceitável, com base nas diretrizes estabelecidas pelas Normas NBR ISO IEC 27001:2013 e NBR ISO IEC 27002:20130.

4.3. A REAL GRANDEZA deve prover uma estrutura de privacidade e proteção de dados pessoais nos sistemas de Tecnologia da Informação com base nas diretrizes estabelecidas pela Norma NBR ISO IEC 29100:2020.

4.4. A REAL GRANDEZA deve cumprir com suas responsabilidades e obrigações de segurança de dados pessoais de acordo com a Lei nº 13.709/2018, denominada Lei Geral de Proteção de Dados Pessoais (LGPD);

4.5. A REAL GRANDEZA deve preservar e proteger as informações sob a responsabilidade, inclusive as contidas nos recursos de Tecnologia da Informação, dos diversos tipos de ameaça e desvios de finalidade em todo o seu ciclo de vida, estejam elas em qualquer suporte ou formato.

4.6. A REAL GRANDEZA deve prevenir e mitigar impactos gerados por incidentes envolvendo a segurança da informação e comunicação.

4.7. A REAL GRANDEZA deve cumprir a legislação vigente no Brasil e demais instrumentos regulamentares relacionados às atividades da entidade no que diz respeito

à segurança da informação, aos objetivos institucionais e aos princípios de privacidade, morais e éticos.

4.7. Quanto à Segurança da Informação:

4.7.1. Segurança da Informação é um assunto complexo e abrangente que depende de pessoas, tecnologias e processos, exigindo profissionais dedicados e especializados, para assegurar a sua implementação, garantindo a manutenção de um nível de segurança aceitável e adequado às necessidades e requisitos da informação da REAL GRANDEZA, evitando prejuízos financeiros ou de imagem, bem como prevenindo sua utilização, intencional ou não, para fins ilícitos.

4.7.2. Nesse sentido, deve ser dado enfoque especial à certificação digital, como forma de verificação da autenticidade de documentos digitais e segurança das transações realizadas através de redes de computadores.

4.7.3. Para minimizar os riscos de segurança na infraestrutura tecnológica corporativa, é necessário também que cada área de negócio apresente suas necessidades de segurança em seus processos e que todas as partes interessadas, interligadas entre si através desta infraestrutura, sigam os padrões estabelecidos.

4.7.4. A Política de Segurança da Informação requer a implementação de monitoramento eletrônico e/ou visual de todas e quaisquer tecnologias da informação e/ou comunicação, inclusive monitoramento de uso da Internet e de correio eletrônico, em equipamentos pertencentes ou não à REAL GRANDEZA, desde que ligados à rede ou de efetivo interesse para os objetivos da Entidade, de acordo com os critérios previstos e/ou requeridos na política e nos normativos e documentos a ela associados ou interligados.

4.7.5. As credenciais de acesso, conta de usuário e senha, são mecanismos fundamentais de autenticação nos sistemas da REL A GRANDEZA. Portanto cada usuário é exclusivamente responsável por todas as suas senhas de acesso, que são pessoais, intransferíveis e de uso exclusivo do usuário, que assume integral responsabilidade pelo uso indevido por terceiros e compromete-se a mantê-las em sigilo e guardá-las em segurança.

4.8. Quanto ao Uso dos Recursos Tecnológicos:

4.8.1. A REAL GRANDEZA deve instituir sua rede corporativa com o objetivo de interligar todas as áreas de negócios, viabilizar a sua Intranet, serviços de videoconferência, hospedagem de *websites* e permitir o acesso unificado à Internet e ao correio eletrônico, visando a otimização dos recursos e a agilização dos processos administrativos.

4.8.2. A REAL GRANDEZA pode instituir redes com propósito específico de atender determinada área de negócio, tendo em vista as particularidades do caso.

4.8.3. A REAL GRANDEZA deve instituir seu serviço de correio eletrônico visando unicamente a otimização dos recursos e o apoio dos processos administrativos.

4.8.4. Toda informação gerada, armazenada ou veiculada na REAL GRANDEZA é de propriedade desta, reservando-se o direito de monitorar e registrar o seu uso.

4.8.5. O uso de equipamentos que não pertencem à REAL GRANDEZA para desempenho de atividades relacionadas à Entidade – BYOD - atenderá às diretrizes desta Política, podendo ser regulamentado em normativos e/ou procedimento próprio.

4.8.6 Equipamentos de TI quando não puderem ser utilizados para o fim a que se destina devido à perda de suas características, obsolescência ou em razão da inviabilidade econômica de sua recuperação, deverão ser encaminhados para a baixa patrimonial e posterior descarte/doação. A GTI deverá garantir a completa exclusão de dados nos equipamentos descartados / doados.

4.9. Quanto à Classificação e o Tratamento da Informação:

4.9.1. A definição do grau de sensibilidade para a informação sensível deve possibilitar:

a) a determinação de medidas mínimas para proteger tais informações; e

b) a garantia da continuidade operacional de processamento destas informações.

4.9.2. As informações documentadas devem ser identificadas, armazenadas, transmitidas e descartadas de acordo com sua classificação.

4.9.3. Ativos tecnológicos devem ter controles aplicados para a proteção da informação que armazena, processa e manuseia, com o tratamento apropriado à sensibilidade e criticidade operacional, conforme classificada.

4.9.4. O grau de sensibilidade da informação deve ser avaliado quanto à necessidade de proteger a CID - Confidencialidade, Integridade, Disponibilidade da informação.

4.9.5. Classificação da informação quanto ao sigilo:

Pública	**Corporativa**	**Confidencial**
Inexistente	Baixo	Alto
Pode ser divulgada a qualquer pessoa sem que haja implicações à REAL GRANDEZA. O conhecimento desta informação pelo público não expõe a organização a prejuízo financeiro, constrangimento, tampouco compromete a segurança dos ativos.	São restritas ao âmbito da REAL GRANDEZA. Porém, se ocorrer divulgação externa das informações ou comprometimento, as consequências não são críticas.	Informações que a REAL GRANDEZA ou os demais agentes têm a obrigação legal, regulamentar ou social de proteger.

4.10. Quanto à Formulação do Plano de Contingência, Segregação de Funções e Continuidade das Operações:

4.10.1. A REAL GRANDEZA deve instituir conceitos e ações para os planos de contingência aos sistemas computacionais, infraestrutura de rede e servidores existentes, visando obter o conhecimento dos elementos que impactam direta ou indiretamente sobre cada serviço, levando-se em conta a pontuação dos mesmos de acordo com a criticidade e para a segregação de funções entre os usuários e administradores dos sistemas, garantindo sua integridade e segurança, inclusive dos dados armazenados, devendo os órgãos de governança e gestão da Entidade zelar pela exatidão e consistência das informações cadastrais, por meio de procedimentos de atualização e verificação das informações fornecidas.

4.10.2. A contingência pode ser classificada em média (aceitável a disponibilidade em horário comercial, podendo ser interrompida eventualmente), alta (requerida disponibilidade 07 (sete) dias x 24 (vinte e quatro) horas, podendo ser interrompida eventualmente) e altíssima (requerida disponibilidade 07 dias x 24 horas sem interrupções).

4.11. Quanto à Terceirização de Serviços:

4.11.1. A demanda por serviços de TI na REAL GRANDEZA é significativa, tornando-se necessária a tomada de decisão sobre o que terceirizar ou o que desenvolver com a equipe interna.

4.11.2. Portanto, antes de optar pela terceirização de serviços ou não, a Gerência de Tecnologia da Informação - GTI deve emitir relatório técnico apontando as vantagens e desvantagens de cada alternativa, levando em consideração as condições da REAL

GRANDEZA e o caráter eventual da contratação de terceiros, bem como os seguintes aspectos:

a) Critérios para avaliação da empresa a ser contratada, quanto à solidez, experiência e idoneidade e inexistência de conflitos de interesse com a REAL GRANDEZA;

b) Criticidade do serviço para ser confiado a um terceiro, ou seja, se a sua descontinuidade ou interrupção tem impacto na missão da REAL GRANDEZA, sua imagem ou seus processos de negócio;

c) Possibilidade e viabilidade de reter os códigos fontes da aplicação;

d) Previsão de passagem de know-how da empresa contratada para a equipe interna;

e) Valor que a terceirização pode agregar ao serviço, além da redução de custo e de prazo;

f) Retorno sobre o investimento;

g) Necessidade de acesso a conhecimentos especializados e de adotar tecnologias emergentes;

h) Rotatividade dos técnicos, a dificuldade de atrair pessoal qualificado e de retê-los;

i) Tipo de atividade a ser terceirizada; e

j) No caso de optar pela terceirização, sempre que possível, os códigos fontes deverão ser de propriedade da REAL GRANDEZA.

4.11.3. Quando da prestação de serviços por terceiros, no contrato deve estar explicitado quais as responsabilidades da empresa e as atitudes que ela deverá seguir se houver problemas com a equipe técnica, se os resultados forem dúbios ou se os técnicos alocados ao serviço não atenderem ao perfil definido para a atividade a ser desenvolvida. É obrigação do prestador de serviços reportar formalmente à REAL GRANDEZA, qualquer risco de quebra de segurança ou sigilo.

4.12. Quanto aos Sistemas Legados:

4.12.1. No que concerne aos sistemas legados, a diretriz é no sentido de manter os que estão funcionando eficientemente preservando os investimentos já realizados, no entanto atualizando-os tecnologicamente quando necessário, visando adequá-los às novas necessidades dos usuários.

4.12.2. Os sistemas legados, sempre que possível, devem ser revisados de maneira a garantir sua atualização tecnológica e uma integração efetiva com os sistemas e os bancos de dados com os quais tem interface.

4.13. Quanto à Padronização:

4.13.1. A REAL GRANDEZA, com base no princípio da padronização e em estudos realizados por equipe técnica, poderá adotar padrões com os seguintes objetivos:

a) Elevar a produtividade e facilitar a qualificação de mão de obra;

b) Otimizar o uso dos recursos, reduzir custos de manutenção, assistência técnica e suporte;

c) Garantir compatibilidade técnica e desempenho;

d) Assegurar o compartilhamento de informações, principalmente em nível gerencial;

e) Garantir agilidade e eficiência nos processos;

f) Garantir a interoperabilidade dos sistemas e *softwares* e da infraestrutura de *hardware* e redes, e

g) Atender à relação custo-benefício e aos princípios de economicidade.

4.14. Quanto ao Governo Eletrônico:

4.14.1. O Governo Eletrônico configura-se como uma nova relação baseada no uso intensivo das Tecnologias da Informação e Comunicação - TIC, principalmente da Internet, entre os órgãos de governança e os cidadãos, destacando-se os membros dos órgãos estatutários, membros dos comitês, integrantes de Grupos de Trabalho, Comissão de Ética, empregados, participantes, assistidos, patrocinadores, instituidores, fornecedores de produtos e serviços, prestadores de serviços de saúde, autoridades e outras partes interessadas.

4.14.2. As áreas de negócio devem, portanto, priorizar a divulgação de informações atualizadas e de prestação de serviços ao público por meio da Internet e das demais formas de interação eletrônica1, visando aumentar a produtividade da REAL GRANDEZA.

4.14.3. As ações para a inclusão digital na REAL GRANDEZA visam também contribuir com a inclusão social[2] de seus membros dos órgãos estatutários, comitês,

[1] Formas eletrônicas de interagir, tais como: e-mail (correio eletrônico); internet; whatsapp (serviços de mensagens curtas), entre outras formas.

[2] É um conjunto de meios e ações que combatem a exclusão aos benefícios da vida em sociedade, provocada pela falta de classe social, origem geográfica, educação, idade, existência de deficiência ou preconceitos raciais.

integrantes dos Grupos de Trabalho, Comissão de Ética, empregados, participantes e assistidos, devendo para isto não só disponibilizar acesso à rede Internet, mas, principalmente, incluí-los em um contexto tecnológico[3] com aplicação direta nas suas atividades.

4.15. Quanto à Gestão da Informação

4.15.1. A gestão da informação, incluindo a gestão de informação em tecnologia da informação, bem como do conhecimento corporativo de tecnologia da informação será feita por meio da elaboração de normativos e procedimentos de classificação de informação da REAL GRANDEZA.

4.15.2. O tratamento da informação compreenderá todos os meios e processos utilizados para lidar com a informação ao longo de cada fase de seu ciclo de vida, contemplando o conjunto de ações referentes à produção/recepção, classificação propriamente dita, armazenamento, transporte/transmissão/distribuição e o eventual arquivamento ou descarte da informação.

4.15.3. Normativos e procedimentos de classificação da informação aplicar-se-ão a todos os dados e/ou informações criados, coletados, armazenados ou processados pela REAL GRANDEZA, em formato eletrônico ou não, bem como por gravação de voz.

4.16. Quanto às Particularidades da Área de Saúde:

4.16.1. Na gestão de planos de saúde a REAL GRANDEZA sempre deve buscar se adequar às melhores práticas de segurança, preservando a integridade, disponibilidade e confidencialidade dos dados dos beneficiários, atendendo aos regulamentos e às instruções da Agência Nacional de Saúde Suplementar - ANS e demais entidades com competência regulamentar sobre planos de saúde.

4.16.2. A REAL GRANDEZA pode aprovar procedimentos e normativos para definir diretrizes e estabelecer critérios específicos para segurança na gestão de planos de saúde, visando à padronização de processos, a proteção de dados e de informações pessoais, e a adequação aos normativos e regulamentos vigentes.

4.17. Quanto à Estrutura Normativa da Segurança da Informação:

4.17.1. A estrutura normativa da segurança da informação da REAL GRANDEZA deve ser composta por um conjunto de documentos com 03 (três) níveis hierárquicos distintos, a saber:

a) Política de Tecnologia e Segurança da Informação - documento que define a estrutura e as diretrizes referentes à Segurança da Informação;

[3] Nome dado a um grupo de variáveis contextuais com influência no desempenho e na atividade de uma empresa ou organização e traduz o progresso técnico da sociedade, o qual condiciona as inovações ao nível dos processos produtivos e dos produtos.

b) Normativos de segurança da informação - estabelecem obrigações e critérios gerais definidos de acordo com as diretrizes da Política de Segurança da Informação e de políticas correlatas; e

c) Procedimentos de Segurança da Informação - instrumentalizam o disposto na política e nos normativos de segurança da informação, orientando a aplicação em relação às atividades da REAL GRANDEZA.

4.18. Quanto às Fontes de Recurso e Cooperação:

4.18.1. Para a concretização de todos os programas e projetos de TI no âmbito da REAL GRANDEZA, deve ser elaborado um planejamento orçamentário de investimento e estrutural, alinhado ao Planejamento Estratégico e ao Plano de Metas e Ações.

4.18.2. Além de recursos financeiros, também deve ser estimulada a busca de cooperação e parceria com universidades, instituições de pesquisa e desenvolvimento, como também com outras entidades e organismos, tanto públicas quanto privadas, para a concretização das diversas ações.

4.19. Quanto ao Processo Disciplinar:

4.19.1. Os membros dos órgãos estatutários, membros dos comitês, integrantes dos Grupos de Trabalho, Comissão de Ética, empregados, estagiários ou jovens aprendizes da REAL GRANDEZA deve cumprir todas as disposições constantes da presente Política. Desta forma, o não cumprimento será considerado uma infração.

4.19.2. As infrações são classificadas em 3 (três) níveis: Leve, Médio e Grave, de acordo com o grau de severidade da tabela abaixo:

Severidade	Impacto
Grave	Impacto imediato no negócio e sem solução alternativa ou temporária. Sistema Crítico ou rede inoperante com alto impacto nas operações da REAL GRANDEZA
Médio	Baixo Impacto imediato no negócio ou solução alternativa disponível. Sistema, aplicativo ou rede com desempenho deteriorado, impactando as operações da REAL GRANDEZA
Leve	Nenhum Impacto no negócio. Sistema, aplicativo ou rede de menor criticidade inoperante, com algum impacto operacional ou com desempenho deteriorado, mas sem impacto imediato no fornecimento dos serviços da REAL GRANDEZA

4.19.3. Diante da constatação de uma infração já devidamente classificada, as sanções serão aplicadas conforme disposto no item 3.2.1. - Penalidades Disciplinares do módulo Normativo Comportamento e Disciplina.

4.19.3.1. No caso de empregado terceirizado, será solicitado, à empresa prestadora da respectiva mão de obra, o afastamento temporário ou definitivo do empregado, conforme a falta cometida podendo, em último caso, a REAL GRANDEZA solicitar a rescisão do contrato de prestação de serviço.

4.19.3.2. A violação de disposição dessa política por membros dos órgãos estatutários, membros de comitês, integrantes de Grupos de Trabalho e Comissão de Ética sujeitará o infrator à penalidade de natureza disciplinar fixada pelo Conselho Deliberativo, conforme regulamentação interna

4.19.4. A aplicação destas sanções não isenta o membro dos órgãos estatutários, membro dos comitês, integrantes dos Grupos de Trabalho, Comissão de Ética, empregado, estagiário ou jovem aprendiz, de sofrer outras penalidades previstas em contrato, ou mesmo de sofrer processos penais por crimes de condescendência criminosa, de violação de sigilo funcional entre outros, estabelecidos no código penal.

4.20. Quanto à Avaliação e Controle dos Riscos

4.20.1. Os riscos relacionados à Segurança da Informação devem ser constantemente avaliados. Deve ser realizada a adequação dos mecanismos de segurança relacionados à liberação de dados sensíveis, de serviços críticos e à troca de informações.

4.20.2 Os gestores devem ser, permanentemente, orientados quanto à identificação dos pontos de controle necessários à manutenção da segurança local e segurança de acessos remotos, incluindo serviços de computação em nuvem.

4.20.3. Em caso de necessidade de utilização de programas e aplicativos específicos de uma determinada atividade, bem como a necessidade de alteração de configuração dos computadores, a área de negócio deverá solicitar formalmente à GTI por meio de documento com justificativa da necessidade e aprovação do diretor responsável pelo processo.

5. RESPONSABILIDADES / ATRIBUIÇÕES

5.1. Gerência de Tecnologia da Informação - GTI

5.1.1.Supervisionar tecnicamente os programas de tecnologia da informação das áreas de negócios, em especial quanto à compatibilidade das propostas com as prioridades e os sistemas utilizados e, em conjunto com a Assessoria de Planejamento e Controle Estratégico - APC, interagindo com os demais gestores no planejamento e no orçamento de projetos de TI, respeitadas as competências previstas nesta política.

5.1.2. Sempre que solicitada, prestar o suporte necessário à Diretoria-Executiva na aprovação de normativos e procedimentos relacionados à área de TI.

5.1.3. Periodicamente avaliar o nível de segurança exigido, o qual dependerá do grau de criticidade e sensibilidade dos dados a serem trafegados por meio da rede corporativa e tomar as medidas necessárias para garantir a segurança desta.

5.1.4. Após a implementação de padrões, continuar acompanhando os efeitos da padronização, avaliando os resultados obtidos e procedendo a reavaliações periódicas para justificar ou não a manutenção dos padrões adotados.

5.1.5. Avaliar a possibilidade de utilização de *software* livre, levando em consideração uma análise de custo-benefício, considerando não somente o custo das licenças, mas sim o custo total de adoção da solução de *software* (incluindo customização, implantação, treinamento, suporte, consultoria, entre outros fatores), e principalmente o critério da segurança da informação.

5.1.6. Orientar os gestores, em conjunto com a Assessoria de Compliance e Riscos - ACR, quanto à identificação dos pontos de controle necessários à manutenção da segurança local e segurança de acessos remotos, incluindo serviços de computação em nuvem.

5.2. Gerência de Recursos Humanos - GRH

5.2.1. As questões relativas ao desenvolvimento e disponibilidade dos gestores de tecnologia da informação serão tratadas em tópico específico do Módulo Normativo de Treinamento, de responsabilidade da Gerência de Recursos Humanos - GRH.

5.2.2. Aplicar ao empregado, estagiário ou jovem aprendiz as medidas disciplinares conforme disposto no item 3.2.1. - Penalidades Disciplinares do módulo Normativo Comportamento e Disciplina.

5.3. Assessoria de Compliance e Riscos - ACR

5.3.1. Interagir, com os gestores de TI, para avaliar os riscos, verificar mecanismos de segurança adequados à liberação de dados sensíveis, de serviços críticos e à troca de informações.

5.3.2. Orientar os gestores, em conjunto com a GTI, quanto à identificação dos pontos de controle necessários à manutenção da segurança local e segurança de acessos remotos, incluindo serviços de computação em nuvem.

5.4. Diretoria Executiva - DE

5.4.1. Aprovar, com o apoio da GTI, o perfil básico para as estações de trabalho específico por atividade.

5.4.2. Aprovar normativos e procedimentos relacionados à classificação da informação, segurança de dados sensíveis, e outros que se fizerem necessários.

5.5. Comitê de Segurança da Informação

5.5.1. Orientar e avaliar as atividades relativas à Segurança da Informação na REAL GRANDEZA, em benefício exclusivo dos negócios corporativos.

5.5.2. Assessorar a Diretoria Executiva na implementação desta Política e elaborar os normativos e procedimentos específicos de segurança da informação**.**

6. DISPOSIÇÕES GERAIS

6.1. O correio eletrônico é de uso exclusivo para fins corporativos, não sendo permitida sua utilização para envio de mensagens com conteúdo de outros fins, dentre os quais: cunho político, religioso ou pornográfico, bem como para envio de mala direta, publicidade comercial ou não, e anúncios.

6.2. O uso do serviço de e-mail para a propagação de mensagens em cadeia é de propriedade exclusiva para mensagens institucionais da REAL GRANDEZA, sendo vedado seu uso para outros fins, independente da vontade do destinatário em receber tais mensagens.

6.3. É vedada a utilização do *software* de acesso à Internet (*browser*) para fins que não sejam de interesse da REAL GRANDEZA, bem como o fornecimento de informações pessoais em sites acessados (“WWW”), informações essas que podem ser posteriormente utilizadas para finalidades indevidas, como o envio de propaganda ou *spam*.

6.4. Para publicações em redes sociais pessoais, deve ser observado o disposto no Art. 8º, inciso III, alínea d do Código de Conduta e Ética.

6.5. A designação de pessoal responsável por atividades de administração de sistemas computacionais e da infraestrutura de *software* e *hardware*, deve ser bastante criteriosa por tratar-se de funções críticas que envolvem informações sigilosas e estratégicas para a REAL GRANDEZA, que necessitam ter integridade, disponibilidade e confidencialidade.

6.6. O membro dos órgãos estatutários, membro dos comitês, integrantes de Grupos de Trabalho, Comissão de Ética, empregado, estagiário ou jovem aprendiz da

REAL GRANDEZA, em qualquer nível hierárquico, na sua esfera de competência, será responsável por cumprir e fazer cumprir a aplicação eficaz dos normativos e princípios decorrentes desta Política, no compromisso com os critérios legais e éticos que envolvem a Entidade. É de sua responsabilidade qualquer prejuízo ou dano que vier a sofrer ou causar à REAL GRANDEZA ou a terceiros, em decorrência de não obediência às diretrizes e normativos referidos.

6.7. Toda informação disponibilizada a um membro dos órgãos estatutários, membro dos comitês, integrantes de Grupos de Trabalho, Comissão de Ética empregado, estagiário ou jovem aprendiz será de uso restrito e confidencial, a menos que o gestor da informação a torne disponível explicitamente para outros usuários ou grupos de usuários, onde a informação disponibilizada será devidamente tratada de acordo com o Módulo Normativo "Classificação de Informações", que deve prever termos de confidencialidade diferenciados conforme a criticidade das funções e/ou das informações das áreas ou grupo de funcionários.

6.8. A divulgação de informação em nome da REAL GRANDEZA somente poderá ser feita por membro dos órgãos estatutários, membro dos comitês, empregado, devidamente autorizado.

6.9. O Comitê de Segurança da Informação, instituído pela Diretoria Executiva, deve ter a seguinte composição: 1 (um) representante da Gerência de Tecnologia da Informação - GTI (Coordenador); 1 (um) representante da Assessoria de Planejamento e Controle Estratégico; 1 (um) representante da Assessoria de Compliance e Riscos - ACR, 1 (um) representante da Gerência de Recursos Humanos – GRH, 1(um) representante da Assessoria jurídica - AJR e o Encarregado de Proteção de Dados da REAL GRANDEZA.

6.10. Esta Política deve ser revisada a cada 03 (três) anos, a partir da data de aprovação pelo Conselho Deliberativo, ou sempre que necessário.

6.11. Casos omissos, não previstos nesta Política, devem ser submetidos ao Conselho Deliberativo para orientação e providências cabíveis.

6.12. Esta Política entra em vigor na data da sua aprovação pelo Conselho Deliberativo