REAL GRANDEZA
Fundação de Previdência e Assistência Social

Proposta de Resolução do Conselho Deliberativo

PRC Nº 049.2015 Data: 22.10.2015

ASSUNTO: Revisão da Política de Tecnologia e Segurança da Informação da REAL GRANDEZA

PROPONENTE: Diretoria Executiva

Proposta: Aprovar a revisão da Política de Tecnologia e Segurança da Informação da REAL GRANDEZA, conforme anexo

Justificativa: Considerando a evolução dos cenários de tecnologia da informação, a implementação do Projeto de Unificação da Gestão dos Planos de Saúde e as recomendações da Auditoria da Patrocinadora FURNAS, se faz necessária a revisão da Política de Tecnologia e Segurança da Informação da REAL GRANDEZA.

Anexo: RDE 001/1096, de 22.10.2015.

Proponente _____
Aristides Leite França
Diretor-Presidente

REAL GRANDEZA
Fundação de Previdência e Assistência Social

Resolução da Diretoria Executiva

RDE Nº 001/1096
1/1

A Diretoria Executiva da REAL GRANDEZA - Fundação de Previdência e Assistência Social na 1096ª reunião, realizada em 22.10.2015, resolveu, a partir da PRDE nº 168.2015:

Aprovar, no seu âmbito de competência, e submeter ao Conselho Deliberativo para aprovação final, a revisão da Política de Tecnologia e Segurança da Informação da REAL GRANDEZA.

Aristides Leite França
Diretor-Presidente

REVISÃO DA PSI – OUTUBRO/2015

DE – PARA

Antes	Depois	Justificativa
	1. INTRODUÇÃO 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 seus empregados, participantes, assistidos, patrocinadores, instituidores, fornecedores de produtos e serviços, autoridades e outras partes interessadas, devendo ser aplicada a todos os sistemas de informação e processos corporativos.	Item incluído em atendimento ao padrão da FRG para a elaboração de normas e políticas.
1. OBJETIVO	**2. OBJETIVO**	Renumerado
2. PREMISSAS A tecnologia da informação por si só não constitui um fim, ..., tendo como premissas básicas: • Gestão estratégica da informação; • Gestão da TI centralizada e com controle integrado; • Informações confiáveis para a tomada de	~~**2. PREMISSAS**~~ **3. PRINCÍPIOS** A tecnologia da informação por si só não constitui um fim, ..., tendo como premissas básicas: • Gestão estratégica da informação; • Gestão da TI centralizada e com controle integrado; • Informações confiáveis para a tomada de	

decisões; • Otimização de recursos; • Inclusão Digital[1]; • Integração dos sistemas de informação e infraestrutura computacional; • Confiabilidade, integridade e disponibilidade de dados; • Foco no cliente interno e externo; • Inovação dos processos com informatização, desburocratização e racionalização; • Melhoria contínua dos processos, sistemas e serviços; • Recursos financeiros adequados; • Pessoal qualificado e continuamente capacitado; • Adequação e atendimento aos padrões da norma técnica, Tecnologia da Informação - Técnicas de Segurança - Código de prática para a gestão da segurança da informação; • Assegurar integridade, confiabilidade e autenticidade das informações sobre os dados financeiros e atuariais do Plano,	decisões; • Otimização de recursos; • Inclusão Digital[2]; • Integração dos sistemas de informação e infraestrutura computacional; • Confiabilidade, integridade e disponibilidade de dados; • Foco no cliente interno e externo; • Inovação dos processos com informatização, desburocratização e racionalização; • Melhoria contínua dos processos, sistemas e serviços; • Recursos financeiros adequados; • Pessoal qualificado e continuamente capacitado; • Adequação e atendimento aos padrões da norma técnica ABNT NBR ISO/IEC 27001:2013, Tecnologia da Informação - Técnicas de Segurança - Código de prática para a gestão da segurança da informação; • Assegurar integridade, confiabilidade e autenticidade das informações sobre os	- Inclusão da Norma Técnica de Segurança da Informação.

[1] Nome dado ao processo de democratização do acesso às tecnologias da Informação, de forma a permitir a inserção de todos na sociedade da informação

[2] Nome dado ao processo de democratização do acesso às tecnologias da Informação, de forma a permitir a inserção de todos na sociedade da informação

seus custos e objetivos, bem como sobre disponibilidade da situação individual de cada participante; • Gestão de riscos; • Documentar, manter documentado, atualizado e controlar os documentos e registros do Sistema de Gestão de Segurança da Informação; • Estabelecer metodologia de análise e avaliação de riscos que assegurem que tais análises e avaliações produzam resultados comparáveis e reproduzíveis; • Estabelecer a realização de auditorias internas do Sistema de Gestão da Segurança da Informação a intervalos planejados; • Estabelecer ações preventivas e corretivas do Sistema de Gestão de Segurança da Informação.	dados financeiros e atuariais do Plano, seus custos e objetivos, bem como sobre disponibilidade da situação individual de cada participante; • Gestão de riscos; • Documentar, manter documentado, atualizado e controlar os documentos e registros do Sistema de Gestão de Segurança da Informação; • Estabelecer metodologia de análise e avaliação de riscos que assegurem que tais análises e avaliações produzam resultados comparáveis e reproduzíveis; • Estabelecer a realização de auditorias internas do Sistema de Gestão da Segurança da Informação a intervalos planejados; • Estabelecer ações preventivas e corretivas do Sistema de Gestão de Segurança da Informação. Os usuários – empregados atuais ou passados, prepostos, terceiros contratados, gerentes, administradores – são responsáveis pelo bom uso	- Foi recomendação da Consultoria Jurídica especializada a inclusão de explicação onde informe que os usuários são responsáveis pelo bom ou mau uso dos recursos tecnológicos.

	dos recursos tecnológicos aos quais tenham acesso, devendo atender, naquilo que lhe for aplicável, aos termos desta Política.	
3. DIRETRIZES As ações e projetos de TI devem sempre considerar o retorno do investimento, ... diversas áreas de negócios. Esta política se aplica às pessoas e aos recursos administrativos e tecnológicos, de caráter permanente ou temporário, pertencentes às áreas de negócio que compõem a REAL GRANDEZA, deve ser divulgada para todo o pessoal envolvido garantindo que tenham as informações necessárias para cumprir adequadamente o que está determinado.	**4. DIRETRIZES** As ações e projetos de TI devem sempre considerar o retorno do investimento... diversas áreas de negócios. Esta política se aplica às pessoas e aos recursos administrativos e tecnológicos, de caráter permanente ou temporário, pertencentes às áreas de negócio que compõem a REAL GRANDEZA, e deve ser divulgada para todo o pessoal envolvido garantindo que tenham as informações necessárias para cumprir adequadamente o que está determinado.	Renumeração de capítulo e acerto ortográfico.
3.1. Quanto ao Planejamento, Orçamento e Aplicação de Recursos em TI A Gerência de Tecnologia da Informação - GTI deve 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 Controladoria e Planejamento -	-	Item transferido para **5. RESPONSABILIDADES / ATRIBUIÇÕES** **5.1. Gerência de Tecnologia da Informação – GTI** **5.1.1 Quanto ao Planejamento, Orçamento e Aplicação de**

ACP, interagindo com os demais gestores no planejamento e no orçamento de projetos de TI, respeitadas as competências previstas no item 5.		**Recursos em TI** em atendimento ao padrão da Real Grandeza para a elaboração de Normas e Políticas.
3.2. Quanto à Segurança da Informação 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 a utilização, intencional ou não, para fins ilícitos. A Assessoria de Controles Internos – ACI tem o papel de 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 através desta infraestrutura, orientando os gestores de TI quanto à implementação dessas políticas e aos demais gestores quanto à identificação dos pontos de controles necessários para a manutenção da	**4.1. Quanto à Segurança da Informação** 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. ~~A Assessoria de Controles Internos – ACI tem o papel de 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 através desta infraestrutura, orientando os gestores de TI quanto à implementação dessas políticas e aos demais gestores quanto à identificação dos pontos de controles necessários para a manutenção da~~	- Renumeração de capítulo e reformulação de texto. - Parte do texto transferido para o item **5.3. Assessoria de Controles Internos – ACI** **5.3.1. Quanto ao Controle de Riscos**, em atendimento ao padrão

segurança local, respeitadas as competências estabelecidas no item 5. Deverá ser dado enfoque especial à certificação digital, por tratar-se de uma tecnologia que vem sendo crescentemente demandada para garantir a identidade dos usuários, a autenticidade de documentos digitais e a segurança das transações realizadas através de redes de computadores. Para minimizar os riscos de segurança na infraestrutura ..., sigam os padrões estabelecidos. A Política de Segurança da Informação requer a implementação ... e documentos a ela associados ou interligados.	~~segurança local, respeitadas as competências estabelecidas no item 5.~~ Nesse sentido, deverá ser dado enfoque especial à certificação digital, como forma de verificação da identidade dos usuários, a autenticidade de documentos digitais e a segurança das transações realizadas através de redes de computadores, inclusive mediante políticas próprias contendo medidas de administração de contas de acesso de usuários. Para minimizar os riscos de segurança na infraestrutura ..., sigam os padrões estabelecidos. A Política de Segurança da Informação requer a implementação ... e documentos a ela associados ou interligados.	da Real Grandeza de elaboração de Normas e Políticas. - Inclusão de item para adequação da PSI as melhores práticas.
3.3. Quanto ao uso da Rede de Dados A REAL GRANDEZA deverá 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	Retirado	Item transferido para os itens **4.2. Quanto ao uso dos Recursos Tecnológicos** **E** **5. RESPONSABILIDADES / ATRIBUIÇÕES**

administrativos. A Gerência de Tecnologia da Informação – GTI deverá, periodicamente, avaliar o nível de segurança exigido, que dependerá do grau de criticidade e sensibilidade dos dados a serem trafegados através da Rede Corporativa e tomar as medidas necessárias para garantir a segurança da Rede. A utilização de serviços da Rede deve ser considerada para o atendimento do princípio da economicidade e deve estar amparada pela ética, propósitos e objetivos de trabalho da Entidade.		**5.1. Gerência de Tecnologia da Informação – GTI** **5.1.2 Quanto ao Uso da Rede de Dados** em atendimento ao padrão da Real Grandeza de elaboração de Normas e Políticas.
3.4. Quanto ao Uso de Correio Eletrônico A REAL GRANDEZA deverá instituir seu serviço de correio eletrônico visando unicamente a otimização dos recursos e o apoio dos processos administrativos. 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. O uso do serviço de e-mail para a propagação de mensagens em cadeia é de propriedade exclusiva	Retirado	Itens transferidos para **6. DISPOSIÇÕES GERAIS** em atendimento ao padrão da Real Grandeza de elaboração de Normas e Políticas.

para mensagens institucionais da REAL GRANDEZA, sendo vedado seu uso para outros fins, independente da vontade do destinatário em receber tais mensagens. **3.5. Quanto ao Uso de Serviços e Servidores WWW** 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*.		
	4.2. Quanto ao uso dos Recursos Tecnológicos A REAL GRANDEZA deverá 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. A REAL GRANDEZA poderá instituir redes com propósito específico de atender determinada área de negócio, tendo em vista as particularidades do caso.	Novo item que contempla parte dos itens **3.3. Quanto ao uso da Rede de Dados e 3.4. Quanto ao Uso de Correio Eletrônico,** da versão anterior da PSI.

	A REAL GRANDEZA deverá instituir seu serviço de correio eletrônico visando unicamente a otimização dos recursos e o apoio dos processos administrativos. Toda informação gerada, armazenada ou veiculada na Entidade REAL GRANDEZA é de propriedade da mesma, reservando-se a esta o direito de monitorar e registrar o uso da mesma. 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.	- Diretrizes para a utilização de equipamentos móveis.
3.6. Quanto à Formulação de Plano de Contingência, Segregação de Funções e Continuidade das Operações A REAL GRANDEZA deverá instituir conceitos e ações para os Planos de Contingência aos sistemas computacionais, infraestrutura de rede e servidores existentes, ... interrupções).	**4.3. Quanto à Formulação de Plano de Contingência, Segregação de Funções e Continuidade das Operações** A REAL GRANDEZA deverá instituir conceitos e ações para os Planos de Contingência aos sistemas computacionais, infraestrutura de rede e servidores existentes, ... interrupções).	Renumeração de capítulos
3.7. Quanto ao Uso de Estações de Trabalho ou Equipamentos Individuais com Acesso à Dados A Diretoria Executiva, por indicação técnica da Gerência de Tecnologia da Informação – GTI	Retirado	Item transferido para **5. RESPONSABILIDADES / ATRIBUIÇÕES** **5.4. Diretoria Executiva – DE / Gerência de Tecnologia da**

deverá aprovar o perfil básico para as estações de trabalho, específico por atividade. 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 Gerência de Tecnologia da Informação, através de documento com justificativa da necessidade e aprovação do Diretor responsável pelo processo. Toda informação gerada, armazenada ou veiculada na Entidade é de propriedade da REAL GRANDEZA, reservando-se a esta o direito de monitorar e registrar o uso da mesma.		**Informação – GTI**
3.8. Quanto à Terceirização de Serviços A demanda por serviços de TI na REAL GRANDEZA ... equipe interna. Portanto, ...aspectos: (...) Quando da prestação de serviços por terceiros, ... a ser desenvolvida.	**4.4. Quanto à Terceirização de Serviços** A demanda por serviços de TI na REAL GRANDEZA ... equipe interna. Portanto, ...aspectos: (...) Quando da prestação de serviços por terceiros, ... a ser desenvolvida.	Renumeração de capítulos
3.9. Quanto às Aquisições e Contratações de Bens e Serviços de TI A REAL GRANDEZA deverá disponibilizar na Instrução Normativa referente à aquisição de produtos e serviços, instruções específicas a serem seguidas por todas as áreas de negócios, quando	Retirado	Itens transferidos para **6. DISPOSIÇÕES GERAIS** Atendimento ao padrão da Real Grandeza de elaboração de Normas e Políticas.

da aquisição de produtos e serviços de TI.		
3.10. Quanto aos Sistemas Legados No que concerne aos sistemas legados, ... usuários. Os sistemas legados... tem interface.	**4.5. Quanto aos Sistemas Legados** No que concerne aos sistemas legados, ... usuários. Os sistemas legados... tem interface.	Renumeração de Capítulos
3.11. Quanto à Padronização A REAL GRANDEZA, com base no princípio da padronização e em estudos realizados por equipe técnica, poderá adotar padrões com os seguintes objetivos: • Elevar a produtividade e facilitar a qualificação de mão de obra; • Otimizar o uso dos recursos, reduzir custos de manutenção, assistência técnica e suporte; • Garantir compatibilidade técnica e desempenho; • Assegurar o compartilhamento de informações, principalmente em nível gerencial; • Garantir agilidade e eficiência nos processos; • Garantir a interoperabilidade dos sistemas e *softwares* e da infraestrutura de *hardware* e redes. Compete à Gerência de Tecnologia da Informação - GTI, após a implementação de	**4.6. Quanto à Padronização** A REAL GRANDEZA, com base no princípio da padronização e em estudos realizados por equipe técnica, poderá adotar padrões com os seguintes objetivos: • Elevar a produtividade e facilitar a qualificação de mão de obra; • Otimizar o uso dos recursos, reduzir custos de manutenção, assistência técnica e suporte; • Garantir compatibilidade técnica e desempenho; • Assegurar o compartilhamento de informações, principalmente em nível gerencial; • Garantir agilidade e eficiência nos processos; • Garantir a interoperabilidade dos sistemas e *softwares* e da infraestrutura de *hardware* e redes. ~~Compete à Gerência de Tecnologia da Informação - GTI, após a implementação de~~	Renumeração de capítulo e exclusão de parte do texto, que foi transferido para o item **5. RESPONSABILIDADES/ ATRIBUIÇÕES** **5.1. Gerência de Tecnologia da Informação – GTI** **5.1.3. Quanto ao Estabelecimento de Padrões para os Recursos de TI,** em atendimento ao padrão da Real Grandeza de elaboração de Normas e Políticas.

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. A padronização sempre deverá atender à relação custo-benefício e aos princípios de economicidade.	~~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.~~ A padronização sempre deverá atender à relação custo-benefício e aos princípios de economicidade.	
3.12. Quanto ao Uso de Software Livre O uso de software livre já é uma realidade, configurando-se como uma alternativa a ser considerada, pois pode reduzir significativamente os custos com pagamento de licenças de software proprietário, além de possibilitar a adequação do software para a gestão, uma vez que o seu código é aberto. Recomenda-se que o gestor de TI faça 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). Neste contexto, deverão ser identificadas as oportunidades para utilização destes softwares, e, sempre que possível, considerar essa opção.	Retirado	Retirado e substituido por diretriz mais estratégica, conforme item **5.14. Quanto ao Uso de Hardwares, Softwares e Metodologias.** Desta forma a diretriz se apresenta de forma mais estratégica, englobando todos os tipos de SW e HW.

Na adoção de software livre, da mesma forma que para os outros tipos de software, o Gestor de TI deve obrigatoriamente considerar as características e requisitos compatíveis com os adotados para padronização de tecnologias pela REAL GRANDEZA.		
3.13. Quanto ao Quadro Funcional A designação pelos Gerentes, 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. O empregado da REAL GRANDEZA, em qualquer nível hierárquico, na sua esfera de competência, será responsável em cumprir e fazer cumprir a aplicação eficaz das normas 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 as diretrizes e normas referidas. Toda informação disponibilizada a um empregado ou grupo de empregados será de uso	Retirado	Transferido para o item **6. DISPOSIÇÕES GERAIS** **6.5. Quanto ao Quadro Funcional,** em atendimento ao padrão da Real Grandeza de elaboração de Normas e Políticas.

restrito e confidencial, a menos que o Gestor da Informação a torne disponível explicitamente para outros usuários, grupos de usuários ou grupo de empregados, onde a informação disponibilizada será devidamente tratada de acordo com o Plano de Classificação de Sigilo de Informações, que deverá prever Termos de Confidencialidade diferenciados conforme a criticidade das funções e/ou das informações de departamentos ou grupo de funcionários. A divulgação de informação em nome da REAL GRANDEZA somente poderá ser feita por empregado devidamente autorizado.		
3.14. Quanto ao Governo Eletrônico Governo Eletrônico configura-se como uma nova relação..., autoridades e outras partes interessadas. As áreas de negócios devem, ..., visando aumentar a produtividade da REAL GRANDEZA. As ações para a inclusão digital na REAL GRANDEZA ... aplicação direta nas suas atividades.	**4.7. Quanto ao Governo Eletrônico** Governo Eletrônico configura-se como uma nova relação..., autoridades e outras partes interessadas. As áreas de negócios devem, ..., visando aumentar a produtividade da REAL GRANDEZA. As ações para a inclusão digital na REAL GRANDEZA ... aplicação direta nas suas atividades.	Renumeração de capítulo
	4.8. Quanto à Gestão da Informação A gestão da informação, incluindo a gestão de informação em tecnologia da informação, bem como do conhecimento corporativo de tecnologia	Item novo que visa contemplar as questões relativas a Classificação da Informação

	da informação será feita por meio da elaboração de normativos e procedimentos de classificação de informação da REAL GRANDEZA. 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. Normativos e procedimentos de classificação da informação aplicar-se-ão a todos os dados e/ou informação criados, coletados, armazenados ou processados pela REAL GRANDEZA, em formato eletrônico ou não, bem como oralmente.	
	4.9. Quanto às Particularidades da Área de Saúde Na gestão de planos de saúde a REAL GRANDEZA buscará sempre 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 - ANS e demais entidades	Item novo que visa contemplar as questões relativas a área de saúde após o processo de unificação da gestão dos planos na Real Grandeza.

	com competência regulamentar sobre planos de saúde. A REAL GRANDEZA aprovará 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.	
3.15 Quanto a Estrutura da Segurança da Informação A estrutura normativa da Segurança da Informação da REAL GRANDEZA ... 3 (três) níveis hierárquicos distintos, a saber: · **Política de Tecnologia e Segurança da Informação** ... · **Normas de Segurança da Informação** = ...; · **Procedimentos de Segurança da Informação** = ...	**4.10 Quanto a Estrutura da Segurança da Informação** A estrutura normativa da Segurança da Informação da REAL GRANDEZA ... 3 (três) níveis hierárquicos distintos, a saber: · **Política de Tecnologia e Segurança da Informação** ... · **Normas de Segurança da Informação** = ...; · **Procedimentos de Segurança da Informação** = ...	Renumeração de capítulos
3.16. Quanto a Aprovação e Revisão Os documentos integrantes da estrutura normativa da Segurança da Informação da REAL GRANDEZA deverão ser aprovados e revisados (para adaptação ou atualização, periódica ou não) conforme os seguintes critérios:	Retirado	Já está previsto nas normas de elaboração de normas e políticas da Real Grandeza.

· **Política** · Nível de Aprovação = Conselho Deliberativo · Periodicidade de Revisão = Anual · **Normas** · Nível de Aprovação = Diretoria Executiva · Periodicidade de Revisão = Anual · **Procedimentos** · Nível de Aprovação = Diretoria responsável pela área envolvida · Periodicidade de Revisão = Anual		
4. Fontes de Financiamento e Cooperação Para a concretização de todos os programas e projetos de TI no âmbito da REAL GRANDEZA, ..., tanto públicas quanto privadas, para a concretização das diversas ações.	**4.11 Fontes de Financiamento e Cooperação** Para a concretização de todos os programas e projetos de TI no âmbito da REAL GRANDEZA, ..., tanto públicas quanto privadas, para a concretização das diversas ações.	Renumeração de capítulos
	5. RESPONSABILIDADES / ATRIBUIÇÕES **5.1. Gerência de Tecnologia da Informação – GTI** **5.1.1 Quanto ao Planejamento, Orçamento e Aplicação de Recursos em TI** A Gerência de Tecnologia da Informação - GTI deve 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 Controladoria e Planejamento - ACP,	Novo item que contempla as responsabilidades e atribuições de todas as áreas da Real Grandeza. Vale ressaltar que este capítulo foi criado em atendimento ao padrão da Real Grandeza de elaboração de Normas e Políticas.

	interagindo com os demais gestores no planejamento e no orçamento de projetos de TI, respeitadas as competências previstas nesta Política. Sempre que solicitada, a GTI prestará o suporte necessário à Diretoria-Executiva na aprovação de normativos e procedimentos relacionados à área de TI. **5.1.2 Quanto ao Uso da Rede de Dados** A Gerência de Tecnologia da Informação - GTI deverá, periodicamente, avaliar o nível de segurança exigido, que dependerá do grau de criticidade e sensibilidade dos dados a serem trafegados através da rede corporativa e tomar as medidas necessárias para garantir a segurança desta. **5.1.3. Quanto ao Estabelecimento de Padrões para os Recursos de TI** Compete à Gerência de Tecnologia da Informação - GTI, 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. **5.14. Quanto ao Uso de Hardwares, Softwares e Metodologias.** Na adoção de qualquer tipo de *software*, o gestor de TI deve obrigatoriamente considerar as características e requisitos compatíveis com os adotados para padronização de tecnologias pela REAL GRANDEZA. O(s) *software(s)* deverão ser submetidos para aprovação da GTI. **5.2. Gerência de Recursos Humanos – GRH** **5.2.1 – Quanto ao Desenvolvimento e Disponibilidade dos gestores de TI** As questões relativas ao desenvolvimento e disponibilidade dos gestores de tecnologia da informação serão tratadas em tópico específico do Módulo Normativo "Treinamento", de responsabilidade da Gerência de Recursos Humanos - GRH. **5.3. Assessoria de Controles Internos – ACI**	

	5.3.1. Quanto ao Controle de Riscos A Assessoria de Controles Internos - ACI tem o papel de 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 através desta infraestrutura, orientando os gestores de TI quanto à implementação dessas políticas e aos demais gestores quanto à identificação dos pontos de controles necessários para a manutenção da segurança local, segurança de acessos remotos, incluindo serviços de computação em nuvem, respeitadas as competências estabelecidas nesta Política. **5.4. Diretoria Executiva – DE / Gerência de Tecnologia da Informação – GTI** **5.4.1. Quanto ao Uso de Estações de Trabalho ou Equipamentos Individuais com Acesso à Dados** A Diretoria-Executiva, por indicação técnica da Gerência de Tecnologia da Informação – GTI, deverá aprovar o perfil básico para as estações de trabalho, específico por atividade. 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 Gerência de Tecnologia da Informação, através de documento com justificativa da necessidade e aprovação do diretor responsável pelo processo. **5.4.2. Quanto à Aprovação de Normativos e Procedimentos** Como forma de garantir a segurança dos dados e das informações, a Diretoria- Executiva, com o suporte da GTI, aprovará normativos e procedimentos relacionados a classificação da informação, segurança de dados sensíveis, e outros que se fizerem necessários.	
5. DESDOBRAMENTOS DESTA POLÍTICA Cabe ao Comitê de Segurança da Informação, instituído pela Diretoria Executiva, e composto dentre outras, pelas áreas de Tecnologia da Informação, Planejamento, Controles Internos e Recursos Humanos, coordenar, orientar e avaliar as atividades relativas à Segurança da Informação na REAL GRANDEZA, em	**Retirado**	Transferido para o capítulo **6. DISPOSIÇÕES GERAIS** **6.6. Desdobramentos da Política,** onde a revisão passou a ser a cada 3(três) anos.

benefício exclusivo dos negócios corporativos. Esta Política deverá ser revisada a cada ano a partir da data de aprovação pelo Conselho Deliberativo. O Comitê de Segurança da Informação deverá assessorar a Diretoria Executiva na implementação desta Política e elaborar as Normas e Procedimentos específicos de segurança da informação.		
	6. DISPOSIÇÕES GERAIS **6.1. Quanto a Classificação da Informação** Como forma de garantir a segurança dos dados e das informações, a Diretoria- Executiva, com o suporte da GTI, aprovará normativos e procedimentos relacionados a classificação da informação, segurança de dados sensíveis, e outros que se fizerem necessários. **6.2. Quanto ao Uso de Correio Eletrônico** 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	Novo item que contempla passagens da PSI que precisaram ser reposicionadas em atendimento ao padrão da Real Grandeza de elaboração de Normas e Políticas.

	pornográfico, bem como para envio de mala direta, publicidade comercial ou não, e anúncios. 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. Quanto ao Uso de Serviços e Servidores "WWW"** 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. Quanto às Aquisições e Contratações de Bens e Serviços de TI** A REAL GRANDEZA deverá disponibilizar no Módulo Normativo referente à aquisição de produtos e serviços, instruções específicas a	

	serem seguidas por todas as áreas de negócios, quando da aquisição de produtos e serviços de TI. **6.5. Quanto ao Quadro Funcional** A designação pelos gerentes 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. O empregado 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. Toda informação disponibilizada a um	

	empregado ou grupo de empregados será de uso restrito e confidencial, a menos que o gestor da informação a torne disponível explicitamente para outros usuários, grupos de usuários ou grupo de empregados, onde a informação disponibilizada será devidamente tratada de acordo com o Módulo Normativo "Classificação de Informações", que deverá prever termos de confidencialidade diferenciados conforme a criticidade das funções e/ou das informações das áreas ou grupo de funcionários. A divulgação de informação em nome da REAL GRANDEZA somente poderá ser feita por empregado devidamente autorizado. **6.6. Desdobramentos da Política** Cabe ao Comitê de Segurança da Informação, instituído pela Diretoria-Executiva, e composto dentre outras, pelas áreas de Tecnologia da Informação, Planejamento, Controles Internos e Recursos Humanos, coordenar, orientar e avaliar as atividades relativas à segurança da informação na REAL GRANDEZA, em benefício exclusivo dos negócios corporativos. Esta política deverá ser revisada a cada 3(três)	

	anos, a partir da data de aprovação pelo Conselho Deliberativo. O Comitê de Segurança da Informação deverá assessorar a Diretoria- Executiva na implementação desta política e elaborar os normativos e procedimentos específicos de segurança da informação.	

REAL GRANDEZA
FUNDAÇÃO DE PREVIDÊNCIA E ASSISTÊNCIA SOCIAL

Carta Interna

Para: Ana Paula Nogueira Larini - GTI

Data: 16.09.2015

De: Sergio Botto da Cunha Filho - ACI

N.Ref.: ACI.I.062.2015

Assunto: Política de Segurança e Tecnologia da Informação

1. Tendo em vista a carta GTI.I.039.2015, de 27.07.15, referente a Política de Segurança e Tecnologia da Informação, informamos que não temos nenhuma objeção a respeito do conteúdo deste quanto a sua conformidade.

2. Informamos que não analisamos o conteúdo do documento em relação a sua gramática.

3. Para fins de padronização do referido documento, torna-se imperativo que após a aprovação nas respectivas instâncias o mesmo seja submetido a esta Assessoria para as devidas providências.

4. Sem mais para o momento, estamos à disposição para maiores esclarecimentos.

Atenciosamente,

ACI/TMMF

Sergio Botto da Cunha Filho
Assessoria de Controles Internos

REAL GRANDEZA
FUNDAÇÃO DE PREVIDÊNCIA E ASSISTÊNCIA SOCIAL

DA/GTI

POLÍTICA
SEGURANÇA E TECNOLOGIA DA INFORMAÇÃO

Versão: 3

2015

REAL GRANDEZA
FUNDAÇÃO DE PREVIDÊNCIA E ASSISTÊNCIA SOCIAL

DA/GTI

POLÍTICA
SEGURANÇA E TECNOLOGIA DA INFORMAÇÃO

Versão: 3

Aprovado em: XX / XX / 2015

Documento de Aprovação: RC Nº XXX/XXX

SUMÁRIO

1. INTRODUÇÃO

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 seus empregados, participantes, assistidos, patrocinadores, instituidores, fornecedores de produtos e serviços, autoridades e outras partes interessadas, devendo ser aplicada a todos os sistemas de informação e processos corporativos.

2. OBJETIVO

Propiciar o aperfeiçoamento da gestão de informática, estabelecer mecanismos para a segurança das informações 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:

- Promover a informatização dos processos, estimulando a ampla utilização da tecnologia da informação para apoio à gestão e suporte das suas atividades;
- Promover a convergência e integração de redes, serviços e sistemas de informação;
- Maximizar o retorno dos investimentos em TI, com a implantação de projetos eficientes, otimizando a aplicação dos recursos financeiros disponíveis;
- 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;
- Incentivar a utilização de portal corporativo, através da Internet e Intranet, como ferramenta de comunicação com empregados, participantes e assistidos;
- Estimular a utilização de documentação digital, empregando conceitos e técnicas de gestão eletrônica de documentos;
- Padronizar tecnologias, visando a interconexão, integração e intercâmbio de aplicações entre as áreas de negócio, além da redução de custos;
- Observar a Política de Propriedade Intelectual, o Plano de Classificação de Sigilo de Informações, o Plano de Contingência e Continuidade de Operações, os programas de governança corporativa e de governança de tecnologia da informação e o Código de Conduta e Ética da Entidade.

3. PRINCÍPIOS

A tecnologia da informação (TI) por si só não constitui um fim, estando a sua aplicação associada aos processos organizacionais, devendo, portanto, ser utilizada de forma a agregar valor para a REAL GRANDEZA, tendo como premissas básicas:

- Gestão estratégica da informação;
- Gestão da TI centralizada e com controle integrado;
- Informações confiáveis para a tomada de decisões;
- Otimização de recursos;
- Inclusão digital;
- Integração dos sistemas de informação e infraestrutura computacional;
- Confiabilidade, integridade e disponibilidade de dados;
- Foco no cliente interno e externo;
- Inovação dos processos com informatização, desburocratização e racionalização;
- Melhoria contínua dos processos, sistemas e serviços;
- Recursos financeiros adequados;
- Pessoal qualificado e continuamente capacitado;
- Adequação e atendimento aos padrões da norma técnica ABNT NBR ISO/IEC 27001:2013, Tecnologia da Informação - Técnicas de Segurança - Código de prática para a gestão da segurança da informação;
- Assegurar integridade, confiabilidade e autenticidade das informações sobre os dados financeiros e atuariais do plano, seus custos e objetivos, bem como sobre disponibilidade da situação individual de cada participante;
- Gestão de riscos;
- Documentar, manter documentado, atualizado e controlar os documentos e registros do Sistema de Gestão de Segurança da Informação;
- Estabelecer metodologia de análise e avaliação de riscos que assegurem que tais análises e avaliações produzam resultados comparáveis e reproduzíveis;
- Estabelecer a realização de auditorias internas do Sistema de Gestão da Segurança da Informação a intervalos planejados;
- Estabelecer ações preventivas e corretivas do Sistema de Gestão de Segurança da Informação.

Os usuários - empregados atuais ou passados, prepostos, terceiros contratados, gerentes, administradores - são responsáveis pelo bom uso dos recursos tecnológicos aos quais tenham acesso, devendo atender, naquilo que lhe for aplicável, aos termos desta política.

4. DIRETRIZES

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.

Esta política se aplica às pessoas e aos recursos administrativos e tecnológicos, de caráter permanente ou temporário, pertencentes às áreas de negócio que compõem a REAL GRANDEZA, e deve ser divulgada para todo o pessoal envolvido, garantindo que tenham as informações necessárias para cumprir adequadamente o que está determinado.

4.1. Quanto à Segurança da Informação

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.

Nesse sentido, deverá ser dado enfoque especial à certificação digital, como forma de verificação da identidade dos usuários, a autenticidade de documentos digitais e a segurança das transações realizadas através de redes de computadores, inclusive mediante políticas próprias contendo medidas de administração de contas de acesso de usuários.

Para minimizar os riscos de segurança na infraestrutura tecnológica corporativa, é necessário também que cada área de negócio apresente suas necessidades de segurança local e que todas as partes usuárias, interligadas entre si através desta infraestrutura, sigam os padrões estabelecidos. A Política de Segurança e Tecnologia 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 Entidade, desde que ligados à rede da REAL GRANDEZA, ou de efetivo interesse para os objetivos da REAL GRANDEZA, de acordo com os critérios previstos e/ou requeridos na política e nos normativos e documentos a ela associados ou interligados.

4.2. Quanto ao Uso dos Recursos Tecnológicos

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

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

Toda informação gerada, armazenada ou veiculada na Entidade é de propriedade da mesma, reservando-se a esta o direito de monitorar e registrar o uso da mesma.

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.

4.3. Quanto à Formulação de Plano de Contingência, Segregação de Funções e Continuidade das Operações

A REAL GRANDEZA deverá 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.

A contingência poderá 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 (sete) dias x 24 (vinte e quatro) horas sem interrupções).

4.4. Quanto à Terceirização de Serviços

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.

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:

- Critérios para avaliação da empresa a ser contratada, quanto à solidez, experiência e idoneidade e inexistência de conflitos de interesse com a REAL GRANDEZA;
- 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;
- Possibilidade e viabilidade de reter os códigos fontes da aplicação;
- Previsão de passagem de *know-how* da empresa contratada para a equipe interna;
- Valor que a terceirização pode agregar ao serviço, além da redução de custo e de prazo;
- Retorno sobre o investimento;
- Necessidade de acesso a conhecimentos especializados e de adotar tecnologias emergentes;
- Rotatividade dos técnicos, a dificuldade de atrair pessoal qualificado e de retê-los;
- Tipo de atividade a ser terceirizada.

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

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.

4.5. Quanto aos Sistemas Legados

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.

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.

4.6. Quanto à Padronização

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

- Elevar a produtividade e facilitar a qualificação de mão de obra;
- Otimizar o uso dos recursos, reduzir custos de manutenção, assistência técnica e suporte;
- Garantir compatibilidade técnica e desempenho;
- Assegurar o compartilhamento de informações, principalmente em nível gerencial;
- Garantir agilidade e eficiência nos processos;
- Garantir a interoperabilidade dos sistemas e *softwares* e da infraestrutura de *hardware* e redes.

A padronização sempre deverá atender à relação custo-benefício e aos princípios de economicidade.

4.7. Quanto ao Governo Eletrônico

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 empregados, os participantes, os assistidos, os patrocinadores, instituidores, fornecedores de produtos e serviços, autoridades e outras partes interessadas.

As áreas de negócio devem, portanto, priorizar a divulgação de informações atualizadas e de prestação de serviços ao público através da Internet e das demais formas de interação eletrônica[1], visando aumentar a produtividade da REAL GRANDEZA.

As ações para a inclusão digital na REAL GRANDEZA visam também contribuir com a inclusão social[2] de seus 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.

4.8. Quanto à Gestão da Informação

A gestão da informação, incluindo a gestão de informação em tecnologia da informação, bem como do conhecimento corporativo de tecnologia da informação, será

---

[1] Formas eletrônicas de interagir, tais como: email (correio eletrônico); internet; msn (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.

[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.

feita por meio da elaboração de normativos e procedimentos de classificação de informação da REAL GRANDEZA.

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.

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 oralmente.

4.9. Quanto às Particularidades da Área de Saúde

Na gestão de planos de saúde a REAL GRANDEZA buscará sempre 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 - ANS e demais entidades com competência regulamentar sobre planos de saúde.

A REAL GRANDEZA aprovará 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.

4.10. Quanto a Estrutura da Segurança da Informação

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

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

4.11. Fontes de Financiamento e Cooperação

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

Além de recursos financeiros, também deverá 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.

5. RESPONSABILIDADES / ATRIBUIÇÕES

5.1. Gerência de Tecnologia da Informação - GTI

5.1.1. Quanto ao Planejamento, Orçamento e Aplicação de Recursos em TI

A Gerência de Tecnologia da Informação - GTI deve 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 Controladoria e Planejamento - ACP, interagindo com os demais gestores no planejamento e no orçamento de projetos de TI, respeitadas as competências previstas nesta política.

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

5.1.2. Quanto ao Uso da Rede de Dados

A Gerência de Tecnologia da Informação - GTI deverá, periodicamente, avaliar o nível de segurança exigido, que dependerá do grau de criticidade e sensibilidade dos dados a serem trafegados através da rede corporativa e tomar as medidas necessárias para garantir a segurança desta.

5.1.3. Quanto ao Estabelecimento de Padrões para os Recursos de TI

Compete à Gerência de Tecnologia da Informação - GTI, 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.

5.14. Quanto ao Uso de Hardwares, Softwares e Metodologias.

Na adoção de qualquer tipo de *software*, o gestor de TI deve obrigatoriamente considerar as características e requisitos compatíveis com os adotados para

padronização de tecnologias pela REAL GRANDEZA. O(s) *software(s)* deverão ser submetidos para aprovação da GTI.

5.2. Gerência de Recursos Humanos – GRH

5.2.1. Quanto ao Desenvolvimento e Disponibilidade dos Gestores de TI

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

5.3. Assessoria de Controles Internos - ACI

5.3.1. Quanto ao Controle de Riscos

A Assessoria de Controles Internos - ACI tem o papel de 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 através desta infraestrutura, orientando os gestores de TI quanto à implementação dessas políticas e aos demais gestores quanto à identificação dos pontos de controles necessários para a manutenção da segurança local, segurança de acessos remotos, incluindo serviços de computação em nuvem, respeitadas as competências estabelecidas nesta política.

5.4. Diretoria Executiva - DE / Gerência de Tecnologia da Informação - GTI

5.4.1. Quanto ao Uso de Estações de Trabalho ou Equipamentos Individuais com Acesso à Dados

A Diretoria-Executiva, por indicação técnica da Gerência de Tecnologia da Informação - GTI, deverá aprovar o perfil básico para as estações de trabalho, específico por atividade. 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 Gerência de Tecnologia da Informação, através de documento com justificativa da necessidade e aprovação do diretor responsável pelo processo.

5.4.2. Quanto à Aprovação de Normativos e Procedimentos

Como forma de garantir a segurança dos dados e das informações, a Diretoria-Executiva, com o suporte da GTI, aprovará normativos e procedimentos relacionados a classificação da informação, segurança de dados sensíveis, e outros que se fizerem necessários.

6. DISPOSIÇÕES GERAIS

6.1. Quanto a Classificação da Informação

Como forma de garantir a segurança dos dados e das informações, a Diretoria-Executiva, com o suporte da GTI, aprovará normativos e procedimentos relacionados a classificação da informação, segurança de dados sensíveis, e outros que se fizerem necessários.

6.2. Quanto ao Uso de Correio Eletrônico

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.

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. Quanto ao Uso de Serviços e Servidores "WWW"

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. Quanto às Aquisições e Contratações de Bens e Serviços de TI

A REAL GRANDEZA deverá disponibilizar no módulo normativo referente à aquisição de produtos e serviços, instruções específicas a serem seguidas por todas as áreas de negócios, quando da aquisição de produtos e serviços de TI.

6.5. Quanto ao Quadro Funcional

A designação pelos gerentes 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.

O empregado 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.

Toda informação disponibilizada a um empregado ou grupo de empregados será de uso restrito e confidencial, a menos que o gestor da informação a torne disponível explicitamente para outros usuários, grupos de usuários ou grupos de empregados, onde a informação disponibilizada será devidamente tratada de acordo com o módulo normativo "Classificação de Informações", que deverá prever termos de confidencialidade diferenciados conforme a criticidade das funções e/ou das informações das áreas ou grupo de funcionários.

A divulgação de informação em nome da REAL GRANDEZA somente poderá ser feita por empregado devidamente autorizado.

6.6. Desdobramentos da Política

Cabe ao Comitê de Segurança da Informação, instituído pela Diretoria-Executiva e composto - dentre outras - pelas áreas de Tecnologia da Informação, Planejamento, Controles Internos e Recursos Humanos, coordenar, orientar e avaliar as atividades relativas à segurança da informação na REAL GRANDEZA, em benefício exclusivo dos negócios corporativos.

Esta política deverá ser revisada a cada 03 (três) anos, a partir da data de aprovação pelo Conselho Deliberativo.

O Comitê de Segurança da Informação deverá assessorar a Diretoria-Executiva na implementação desta política e elaborar os normativos e procedimentos específicos de segurança da informação.