Políticas Institucionais de

Segurança da Informação e Tecnologia da Comunicação

MARISTA

Apresentação

Melhorar nossos processos de governança e gestão, em todos os níveis da Rede Marista, envolvendo nossos empreendimentos, tem sido um dos nossos principais objetivos, nesses anos à frente da instituição. Os Conselhos têm se preocupado com a busca de políticas institucionais que alinhem as nossas práticas e nos conduzam para melhores resultados, buscando a conformidade na Rede e, em mais ampla escala, a sustentabilidade da missão no longo prazo. Dessa forma, tenho a alegria de apresentar a Política Institucional de Segurança da Informação e Tecnologia da Comunicação da Rede Marista, que envolve as Instâncias Corporativa e Canônica, a Pontifícia Universidade Católica do Rio Grande do Sul, o Hospital São Lucas, o Instituto do Cérebro, os Colégios e as Unidades Sociais.

Essa Política, elaborada por várias mãos, tem a contribuição das experiências e conhecimentos de cada um de nossos empreendimentos e foi validada nos principais espaços de tomada de decisão. Ela versa sobre um tema de vital importância nos dias de hoje: o modo como tratamos as informações e os dados que nos são disponibilizados e que utilizamos para a realização das nossas atividades. Nesse específico, gostaria de chamar a atenção para a importância da ética e do critério no tratamento das informações que

nos são confiadas para a realização de nosso trabalho. Somos uma instituição que tem por base o conhecimento e que se rege pelos valores institucionais, que são inegociáveis. Tratamos, todos os dias, com dados sensíveis da vida de milhares de pessoas que buscam os nossos serviços. Precisamos, por isso mesmo, estar atentos ao que a legislação nos indica e agir de maneira ética, como se espera dos colaboradores maristas.

Tenho certeza de que esta Política, passo importante na busca pela qualidade, transparência, excelência e conformidade, nos ajudará a conduzir melhor os processos que realizamos. Agradeço o empenho de todas as pessoas envolvidas na construção deste documento e de cada um dos profissionais da Rede Marista, que traduzem, no cotidiano, os sonhos e as aspirações de nosso fundador, São Marcelino Champagnat.

A todos, uma abençoada missão!

Ir. Inacio Etges
Presidente/Provincial
Rede Marista/Província Marista Brasil Sul-Amazônia

1 Objetivo

Definir os requisitos relativos à Segurança da Informação e Tecnologia da Comunicação (TIC), bem como os critérios de uso dos recursos tecnológicos, garantindo a prevenção, confidencialidade, integridade, transparência e disponibilidade das informações coletadas, geradas, distribuídas, armazenadas e manipuladas, tratadas nos empreendimentos da Rede Marista, para atender aos requisitos de conformidade às leis vigentes, ao *Código de Conduta do Programa Institucional Nossos Valores,* e às demais normas e boas práticas nacionais e internacionais aplicáveis a esta temática.

2 Abrangência

Todos os Irmãos, colaboradores e contratados em qualquer regime, estudantes, prestadores de serviço, visitantes e qualquer pessoa que porventura possa acessar ou utilizar os recursos de Tecnologia da Informação e Comunicação (TIC) e dados da instituição, independentemente do meio e da finalidade com que são utilizados. Para fins de abrangência, a Rede Marista compreende os empreendimentos Pontifícia Universidade Católica do Rio Grande do Sul (PUCRS), Hospital São Lucas (HSL), Instituto do Cérebro do Rio Grande do Sul (InsCer), Colégios e Unidades Sociais, bem como as áreas corporativa e canônica,

comunidades de Irmãos, centros de eventos e demais empreendimentos vinculados à Rede Marista.

3 Premissas

3.1 Assegurar a continuidade dos serviços necessários para o funcionamento das atividades dos empreendimentos da Rede Marista, no que se refere à segurança de dados e de informações e bom uso das TIC's.

3.2 Buscar a disseminação dos termos desta política, para assegurar a uniformidade da informação.

3.3 Essa política deve ser seguida independentemente do nível hierárquico ou função na Instituição, bem como de vínculo empregatício ou de prestação de serviço.

3.4 O Comitê de Tecnologia da Informação e Comunicação é responsável pelo acompanhamento da implementação e revisão dessa política.

3.5 Deve constar em todos os contratos necessários o anexo de *Acordo de Confidencialidade* e *Proteção de Dados Pessoais* ou *Cláusula de Confidencialidade e Proteção de Dados Pessoais*, como condição imprescindível para que seja concedido o acesso aos ativos de informação disponibilizados pela instituição.

3.6 A responsabilidade em relação à segurança da informação deve ser comunicada na fase de contratação dos colaboradores e prestadores de serviços em cada um dos empreendimentos.

3.7 Os dados e informações produzidos para a gestão e inerentes às atividades profissionais dos empreendimentos devem ser tratados de forma restrita às atividades a que se destinam, não devendo ser divulgados, distribuídos ou disseminados a agentes internos ou externos alheios àquelas informações ou atividades.

3.8 Todos os colaboradores devem ser orientados sobre os procedimentos de segurança, bem como sobre o uso correto dos ativos de informação ou tecnológicos, a fim de mitigar riscos.

3.9 Todo incidente que afete a segurança da informação deve ser imediatamente comunicado à área de tecnologia da informação do respectivo empreendimento e ao encarregado responsável pela proteção de dados pessoais. Caso a área julgue necessário, deve reportar o incidente ao Comitê de Tecnologia da Informação e Comunicação para conhecimento e eventuais providências.

3.10 A Rede Marista poderá buscar a responsabilidade pessoal do agente que, de alguma forma, fizer uso indevido, negligente ou imprudente dos recursos, dados e/ou serviços concedidos aos seus colaboradores, reservando-se o direito de analisar informações e evidências para obtenção de provas a serem

utilizadas em processos investigatórios, bem como adotar as medidas legais cabíveis.

4 Definições

Com base no objetivo da política e nas premissas elencadas, define-se:

4.1 Quanto ao uso da informação:

4.1.1 Toda informação deve ter sua segurança designada e preservada pelos usuários que detêm a sua custódia – sejam eles criadores ou responsáveis designados –, independentemente do meio em que se encontra.

4.1.2 É vedada a utilização de informações para fins pessoais de quem as acessa, bem como para deliberadamente causar dano à imagem em qualquer âmbito da instituição ou de terceiros perante a sociedade.

4.1.3 Todo colaborador deve zelar pela segurança das informações acessadas e utilizadas na execução de suas atividades. Em caso de dúvidas, deverá solicitar orientação às suas lideranças.

4.1.4 Em caso de desligamento de um colaborador, o acesso a dados e recursos de TIC será interrompido.

4.1.5 Não é recomendado o uso de armazenamento local para guarda de arquivos pessoais ou de trabalho. Os arquivos referentes ao

trabalho devem ser armazenados nos espaços disponibilizados e indicados pelos empreendimentos.

4.1.6 As áreas de TIC não mantêm cópia de segurança dos dados pessoais armazenados localmente nas estações de trabalho, fixas ou móveis, não se responsabilizando pela perda das informações e dados armazenados desta forma.

4.1.7 As cópias de segurança das informações armazenadas nos espaços disponibilizados são mantidas pela área de TIC de cada empreendimento.

4.1.8 É vedado ao usuário manipular (acessar, divulgar, excluir, incluir ou alterar) informações elaboradas e/ou mantidas por outros usuários, sem o expresso conhecimento e autorização deles.

4.1.9 Toda e qualquer divulgação de dados ou informações referentes aos empreendimentos, seus negócios e estratégias empresariais, operacionais e institucionais, devem ser tratadas como sigilosas e confidenciais, sendo seu acesso e circulação restritos àquelas pessoas que necessitam conhecê-las para exercer suas atividades.

4.2 Quanto ao uso dos recursos de Tecnologia da Informação e Comunicação (TIC):

4.2.1 Eventuais danos físicos ou lógicos ocorridos aos dispositivos pessoais de qualquer natureza, de propriedade do usuário, enquanto utilizados na estrutura da instituição, serão de responsabilidade única e exclusiva do mesmo.

4.2.2 Os computadores e dispositivos fornecidos pela instituição são disponibilizados com sistema operacional e *software* necessários para a realização da atividade profissional do usuário, de acordo com seu perfil de acesso e cargo que exerce no empreendimento, não sendo permitida a remoção, atualização ou instalação de *software* adicionais, salvo se solicitado e autorizado pela área de TIC.

4.2.3 A aquisição e instalação de *software* adicionais, deverão ser solicitadas pelo líder do usuário à área de tecnologia da informação do empreendimento.

4.2.4 Todos os *software* protegidos por direito autoral deverão ter a respectiva licença de uso corporativo. O uso correto desses *software* é de total responsabilidade do usuário.

4.2.5 Todos os colaboradores deverão observar a legislação brasileira vigente de propriedade intelectual e direito autoral, ficando assim proibida a instalação, armazenamento ou distribuição de

software, músicas, filmes, livros e outros arquivos para os quais os empreendimentos não possuam licença de uso ou direitos adquiridos.

4.2.6 As ferramentas para divulgação de informações, tais como e-mail, *blogs*, fóruns de discussão, *newsletters*, enquetes e publicações em páginas *web,* não poderão ser utilizadas para efetuar a criação ou distribuição de mensagens, com ou sem anexos, que compreendem conteúdo em desacordo com a legislação brasileira vigente e/ou ao *Código de Conduta do Programa Institucional Nossos Valores,* da Rede Marista.

4.2.7 Os equipamentos e plataformas de produção, armazenamento e envio de dados, disponibilizados para a realização das atividades profissionais estão sujeitos a monitoramento remoto e auditoria em qualquer tempo e sobre qualquer pretexto, conforme deliberação institucional.

4.3 Quanto à gestão dos recursos de Tecnologia da Informação e Comunicação:

4.4 É de competência exclusiva da área tecnologia da informação dos empreendimentos as seguintes atividades: instalação, manutenção, auditoria, assessoria na avaliação de necessidades de *software* e *hardware* e análise de contratos relacionadas a recursos e serviços de TIC, em conjunto com outras áreas.

4.5 A área gestora de TIC pode realizar o monitoramento e avaliação contínua da utilização de recursos de TIC visando a garantir a segurança das informações.

4.6 Caso seja identificado pela área de TIC a não observância de algum dos termos desta política pelo usuário, seja de forma intencional, ou não, poderá ser feita a suspensão imediata dos acessos aos recursos de TIC do usuário em questão. A normalização do acesso aos recursos se dará a partir da solicitação da liderança do usuário com apresentação da justificativa.

4.7 Quanto à gestão de acessos e identidades digitais

4.7.1 O usuário é responsável por todas as ações realizadas através de sua conta de acesso à rede e aos recursos de TIC da instituição. O usuário que utilizar privilégios de acesso a sistemas e serviços fornecidos para a execução de atividades que caracterizem conduta criminal será o único responsável por tais atos, sendo direito da instituição buscar a sua isenção de qualquer ônus decorrente de tais atos.

4.7.2 A senha de acesso aos recursos de TIC é pessoal e intransferível, sendo vedado ao usuário divulgá-la a terceiros. Incidentes ocasionados por terceiros a partir da divulgação de qualquer

senha de acesso, propositalmente ou não, serão de responsabilidade de ambas as partes pelos danos causados.

4.7.3 É de responsabilidade da liderança e da área de recursos humanos a avaliação e a concessão de acesso somente a informações e recursos de TIC que sejam pertinentes às atividades profissionais do colaborador.

4.7.4 Em caso de mudança de função, área de atuação ou atividade, as áreas de TIC devem ser comunicadas para adequação do perfil de acesso do usuário em questão.

4.7.5 A qualquer momento, os gestores das áreas poderão solicitar ao setor de TIC, um relatório específico de uso dos recursos computacionais dos usuários de seu setor, conforme disponibilidade técnica.

4.7.6 É vedada a criação de identidades digitais, ou usuários ditos genéricos, que impossibilitem a identificação de um indivíduo nas ações envolvendo recursos computacionais. Abre-se exceção em casos particulares em que tal recurso se faz necessário, a saber:

4.7.6.1 Usuários utilizados para integração entre diferentes sistemas.

4.7.6.2 Usuários com função de administração, requeridos pelos próprios recursos ou sistemas computacionais, tais como o *Active Directory*.

4.7.6.3 Exceções podem ser aplicadas desde que aprovadas pela área de TIC.

4.7.7 Os acessos a recursos computacionais só podem ser disponibilizados mediante solicitação com autorização do gestor da área e/ou Recursos Humanos, e encaminhados ao setor de atendimento de TIC. A solicitação deve informar:

4.7.7.1 Justificativa para acesso.

4.7.7.2 Prazo de utilização, se houver.

4.7.7.3 Nível de acesso do sistema (inclusão / exclusão / alteração).

4.7.7.4 Alçada de acesso (opções do sistema disponíveis para uso).

4.7.8 Deve-se realizar a elaboração de identidades de acesso considerando a boa prática de construção de senhas fortes, envolvendo a inclusão de letras maiúsculas e minúsculas, números e caracteres especiais, atualizadas periodicamente conforme definição do empreendimento.

5.0 Responsabilidades

5.1 Comitê de TIC

5.1.1 O Comitê de Tecnologia da Informação e Comunicação da Rede Marista, composto por representantes dos empreendimentos nomeados pela Presidência da instituição, busca promover a aderência quanto aos parâmetros adotados no que diz respeito à segurança das informações nas unidades de gestão dos empreendimentos.

5.1.2 Manter atualizada a Política Institucional de Segurança da Informação, bem como orientar sobre quaisquer dúvidas decorrentes da sua aplicação.

5.1.3 Dar subsídios à área ou pessoa encarregada de proteção dos dados pessoais do respectivo empreendimento ou da Rede Marista para que esses possam exercer suas atividades em conformidade com a legislação.

5.2 Áreas de Tecnologia da Informação e Comunicação dos Empreendimentos

5.2.1 Zelar pela aplicabilidade desta política.

5.2.2 Avaliar, decidir e reportar sobre eventuais situações que estejam em desacordo ou omissos a esta política.

5.2.3 Identificar e aplicar controles de TIC que assegurem os níveis adequados de segurança da informação.

5.3 Recursos Humanos

5.3.1 Promover o conhecimento da política de segurança da informação e assinatura do termo de responsabilidade do colaborador, parte integrante do Código de Conduta.

5.3.2 Participar e orientar em situações que estejam em desacordo com esta política.

5.3.3 Dar suporte aos colaboradores quanto à aplicação desta política.

6.0 Disposições Finais

6.1 Os casos omissos, bem como ajustes necessários na presente Política, devem ser submetidos à apreciação do Comitê de TIC.

6.2 As demais normativas, que tenham relação com esta política, devem estar adaptadas às definições e procedimentos aqui definidos.

6.3 A não observância dos itens desta política levará à aplicação de ações corretivas por parte da liderança em parceria com a área de recursos humanos.

GLOSSÁRIO

- Segurança da Informação

  É a proteção da informação de vários tipos de ameaças, visando a garantir a continuidade do negócio e a minimização de riscos. São características básicas da segurança da informação os atributos de confidencialidade, integridade e disponibilidade, aplicando-se a todos os aspectos de proteção e tratamento adequado da informação e dos dados.

- Confidencialidade

  Garante que o acesso à informação seja obtido somente por pessoas autorizadas e quando for de fato necessário.

- Integridade

  Garante que a informação seja mantida em seu estado original, visando a protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais.

- Disponibilidade

  Garante que as pessoas autorizadas tenham acesso à informação sempre que necessário.

- Recursos de Tecnologia da Informação e Comunicação

Qualquer sistema de processamento da informação, serviço ou infraestrutura, ou as instalações físicas que os abriguem, como, por exemplo, sistemas informatizados, acessos à internet, intranet e rede interna de dados, computadores, periféricos, notebooks, smartphones, tabletes, software de apoio ao uso administrativo e acadêmico, e correio eletrônico institucional.

- Identidade Digital

Representação digital dos dados relacionados com uma pessoa, empresa, sistema ou máquina, acessível através de dispositivos computacionais. A identidade digital pode incluir dados biográficos (que apresentam registro de informações históricas como nome, endereço, número da segurança social, números de conta, palavras-chave etc.) ou biométricos (que apresentam registro de características físicas ou comportamentais das pessoas como forma de identificá-las unicamente), ou seja, abrange um conjunto de informações atualizadas, organizadas e codificadas em meios digitais.

- Gestão de Identidades

Processo de automatizar e auditar as concessões de acesso a conteúdo digital de uma organização, através de fluxos integrados em uma plataforma centralizada, com procedimentos

automatizados e perfis de acesso de usuários mapeados. Também pode ser definida como o processo de representação, utilização, manutenção, provisionamento e desprovisionamento de identidades digitais, em redes de computadores.

- Encarregado de Proteção de Dados Pessoais

  Pessoa, física ou natural, indicada pela alta administração da Rede Marista ou de seu respectivo empreendimento para agir em conformidade com a legislação acerca do tratamento de dados pessoais tratados por meios físicos ou digitais.

REDE MARISTA / Província Marista Brasil Sul-Amazônia

Presidente/Provincial: Ir. Inacio Nestor Etges

Conselho de Administração/Conselho Provincial: Ir. Deivis Fischer, Ir. Manuir Mentges, Ir. Odilmar Fachi, Ir. Onorino Moresco e Ir. Sandro Bobrzyk

Supervisão Editorial: Comunicação Corporativa

Equipe de Trabalho das Políticas: Carine Moreira, Carlos Heydrian Fonseca Soares, Lucas Braz Ramos, Marcelo Cordeiro, Maurício Testa e Ricardo Ritter.

Revisão técnica: Marcos Másera, Sheila Peixoto e Renato Pereira

Revisão de português: Irany Terezinha Fioravante Dias

Julho de 2019

Sobre a Política: *esta política foi elaborada pelos integrantes do Comitê de TIC da Rede Marista, sob a coordenação do* ***Ir. Odilmar Fachi****, vice-presidente executivo, em julho de 2019. Atualizações e versões da política serão realizadas e disponibilizadas conforme necessidade.*

MARISTA

Rede Marista

Rua Irmão José Otão, 11
Bom Fim - Porto Alegre | RS
CEP: 90035-060
redemarista.org.br