POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

1. INTRODUÇÃO

A Sociedade Mineira de Cultura - SMC, na forma do seu Estatuto, é uma associação civil de fins não econômicos, educacional e beneficente de assistência social. Tem por finalidade, dentre outras, manter instituições de ensino e pesquisa que venham a contribuir para a realização de seus objetivos de instrumento do povo de Deus e difusora de ação missionária da Igreja Católica e da Arquidiocese de Belo Horizonte.

A SMC, as universidades e os colégios mantidos por essa, neste documento denominados simplesmente como SMC e suas unidades mantidas, utilizam a tecnologia e a internet de forma a garantir mais qualidade de ensino para sua comunidade estudantil e acadêmica, sempre a favor do conhecimento e da aprendizagem. No entanto, a mobilidade e a ausência de perímetros físicos e de fronteiras claras que caracterizam a sociedade atual, permitidas pelos avanços tecnológicos, exigem muito mais cuidado para se evitar incidentes que possam colocar em risco os alunos e seus colaboradores.

Nesse contexto, a segurança da informação é uma atividade essencial de proteção de todos os ativos tangíveis e intangíveis da SMC e suas unidades mantidas, a exemplo de imagem, reputação, conhecimento, patrimônio e a própria informação. Desse modo, é fundamental que todos os integrantes, seja na área administrativa ou nos núcleos de docentes ou discentes, pratiquem e disseminem a segurança digital.

Em resposta a essas novas necessidades, está sendo implementado o Sistema de Gestão de Segurança da Informação (SGSI), que possui como diretriz principal a Política de Segurança da Informação (PSI), para atender às peculiaridades do segmento de ensino.

Para que a SMC e suas unidades mantidas alcancem o resultado de proteger seus ativos na produção e compartilhamento de conhecimento, essas novas regras devem ser cumpridas por todos.

2. OBJETIVOS

A Política de Segurança da Informação (PSI) é aplicável ao ambiente estudantil, acadêmico e administrativo e tem por objetivos:

- Estabelecer as diretrizes estratégicas e os princípios para a proteção dos ativos tangíveis e intangíveis, a exemplo da imagem, reputação, marca, propriedade intelectual, bancos de dados e conhecimento, e dos recursos de tecnologia da informação e comunicação (recursos de TIC) da SMC e suas unidades mantidas, além das informações dos alunos;

- Nortear a tomada de decisão e a realização das atividades profissionais e educacionais de todos os colaboradores da SMC e suas unidades mantidas, em ambientes presenciais ou digitais, sempre de acordo com as normas da instituição e a legislação nacional vigente;
- Estabelecer os princípios para o desenvolvimento de atividades educacionais seguras, que afastem danos à reputação da SMC e suas unidades mantidas;
- Construir uma cultura de uso seguro das informações, formando indivíduos mais preparados para agir com responsabilidade e segurança na sociedade digital;
- Preservar a confidencialidade, a integridade, a disponibilidade, a autenticidade e a legalidade das informações e dos recursos de TIC da SMC e suas unidades mantidas;
- Nortear a definição de normas e procedimentos específicos de segurança da informação, bem como a implementação de controles e processos para seu atendimento.

3. ABRANGÊNCIA

Esta PSI é um normativo interno, com valor jurídico e aplicabilidade imediata e irrestrita a todos os alunos e colaboradores, para os ambientes estudantil, acadêmico e administrativo, que venham a ter acesso e/ou utilizam as informações, os recursos de TIC e/ou demais ativos tangíveis ou intangíveis da SMC e suas unidades mantidas.

4. DIRETRIZES GERAIS

4.1 Interpretação

4.1.1 Para efeito desta PSI, são adotados as siglas, os termos e definições constantes no Apêndice A.

4.1.2 Esta PSI deve ser interpretada de forma restritiva, ou seja, casos excepcionais ou que não sejam por ela tratados só podem ser realizados após prévia e expressa autorização da SMC.

4.1.2.1 Qualquer caso de exceção ou permissão diferenciada ocorrerá de forma pontual, aplicável apenas ao seu solicitante, dentro dos limites e motivos que a fundamentaram, cuja aprovação se dará por mera liberalidade da SMC e com

duração limitada, podendo ser revogada a qualquer tempo e sem necessidade de aviso prévio.

4.2 Propriedade

4.2.1 As informações geradas, acessadas, recebidas, manuseadas ou armazenadas, bem como a reputação, a marca, o conhecimento e demais ativos tangíveis e intangíveis da SMC e suas unidades mantidas, são de propriedade e de direito de uso exclusivos de cada unidade.

4.2.2 Os recursos de TIC fornecidos pela SMC e suas unidades mantidas, para o desenvolvimento de atividades estudantis, acadêmicas e profissionais, são de propriedade de cada unidade ou estão a ela cedidos, permanecendo sob sua guarda e posse para uso restrito e, por isso, devem ser utilizados apenas para o cumprimento da finalidade a que se propõem.

4.2.3 Todos os ativos tangíveis e intangíveis da SMC e suas unidades mantidas só podem ser utilizados para o cumprimento das atividades profissionais e educacionais, limitados à função do aluno ou colaborador.

4.2.4 A utilização das marcas, identidade visual e demais sinais distintivos da SMC e suas unidades mantidas, atuais e futuros, em qualquer veículo de comunicação, inclusive na internet e nas mídias sociais, só pode ser feita para atender a atividades profissionais e educacionais, quando prévia e expressamente autorizada.

4.2.5 Todos os alunos e colaboradores poderão fazer menção da marca em conteúdos e materiais, para citação do local onde trabalha, ministra aula ou estuda, mas, em hipótese alguma, poderá a marca ser utilizada para criação de perfis em mídias sociais em nome da instituição e/ou se fazendo passar por ela.

4.3 Classificação da informação

4.3.1 Para que as informações sejam adequadamente protegidas, cabe ao colaborador realizar a classificação no momento em que for gerada a informação, para garantir a devida confidencialidade, especialmente no caso de conteúdos e dados pessoais.

4.3.1.1 Informação pública: informação que pode ou deve ser tornada disponível para distribuição pública. Sua divulgação não causa qualquer dano à instituição e aos alunos.

4.3.1.2 Informação interna: informação que pode ser divulgada para os alunos e colaboradores da instituição, enquanto estiverem desempenhando atividades educacionais e profissionais. Sua divulgação não autorizada ou acesso indevido podem causar impactos institucionais.

4.3.1.3 Informação confidencial: informação exclusiva a quem se destina. Requer tratamento especial. Contém dados pessoais e/ou sigilosos, que, se divulgados, podem afetar a reputação e a imagem da instituição ou causar impactos graves, sob o aspecto financeiro, legal e normativo.

4.3.2 Rotulagem da informação: quando se tratar de informações não públicas, devem ser rotuladas no momento em que forem geradas, armazenadas ou disponibilizadas.

4.3.2.1 Para informações geradas e/ou armazenadas em mídias removíveis ou papel, utilizar carimbo, etiqueta ou texto padronizado para identificação do nível de classificação da informação: interna ou confidencial.

4.3.2.2 Para informações geradas ou mantidas em ambientes lógicos, utilizar documentação específica para definir o nível de classificação da informação, a exemplo de, mas não se limitando a, documento de avaliação de impacto do sistema ou banco de dados, análise de risco do sistema ou banco de dados e Plano Diretor de Segurança, Políticas de Uso.

4.3.3 Em respeito à classificação da informação, todos os alunos e colaboradores devem respeitar o nível de segurança requerido pela classificação indicada na informação que manusear ou com que vier a tomar contato.

4.3.3.1 Em caso de dúvida, todos deverão tratar a informação como de uso interno, não passível de divulgação ou compartilhamento com terceiros ou em ambientes externos à instituição, incluindo a internet e mídias sociais, sem prévia e expressa autorização da SMC e/ou suas unidades mantidas.

4.3.4 Todo colaborador deve respeitar o sigilo profissional e contratual. Por isso, não pode revelar, transferir, compartilhar ou divulgar quaisquer informações confidenciais ou internas, incluindo, mas não se limitando a, informações de outros colaboradores, alunos, fornecedores, prestadores de serviços ou demais detalhes institucionais críticos.

4.3.5 Os alunos devem respeitar o sigilo das informações confidenciais ou internas, incluindo, mas não se limitando a, informações de outros alunos e colaboradores da instituição.

4.3.6 Toda informação envolvendo dados pessoais de alunos, especialmente o prontuário escolar, e de colaboradores deve ser tratada como sigilosa, utilizada com cautela e apenas por pessoas autorizadas.

4.3.7 A GTI é responsável por homologar os mecanismos de criptografia, cifragem ou codificação para o armazenamento e a transmissão de conteúdos confidenciais, quando aplicáveis no desenvolvimento de sistemas internos ou no ambiente de conectividade.

4.4 Controle de acesso

4.4.1 Para cada aluno e colaborador é fornecida uma identidade digital, de uso individual e intransferível, para acesso físico e lógico aos ambientes e recursos de TIC da SMC e suas unidades mantidas.

4.4.1.1 A identidade digital é monitorada e controlada pela SMC e suas unidades mantidas.

4.4.1.2 O aluno e o colaborador são responsáveis pelo uso e o sigilo de sua identidade digital. No caso de uso não autorizado, não é permitido compartilhá-la, divulgá-la ou transferi-la a terceiros.

4.4.2 Quando a identidade for disponibilizada e fornecida pela unidade, todos os colaboradores, prestadores de serviços e visitantes, enquanto presentes nas dependências físicas da instituição, precisam estar devidamente identificados, portando o crachá individual de forma visível.

4.4.2.1 O crachá de identificação é de uso individual, não sendo autorizado o compartilhamento com outro colaborador ou terceiro, tampouco o seu uso fora das dependências da SMC e suas unidades mantidas.

4.4.3 Para a segurança física, a SMC e suas unidades mantidas devem estabelecer espaço físico seguro para proteger as áreas que criam, desenvolvem, processam ou armazenam informações críticas e que contenham ativos críticos para a instituição, a exemplo de, mas não se limitando a, datacenters, sala de Telecom, salas de documentação crítica etc.

4.4.4 Os ativos críticos para a instituição devem estar protegidos contra a falta de energia elétrica e outras interrupções causadas por falhas, além de ter uma correta manutenção para assegurar a sua contínua integridade e disponibilidade.

4.5 Internet

4.5.1 Os recursos de conectividade são fornecidos para atender ao propósito administrativo e educacional, visto que o acesso à internet é um direito essencial para o exercício da cidadania no Brasil. No entanto, os alunos e os colaboradores devem fazer uso da internet em estrita observância das leis em vigor, respondendo pelo seu descumprimento.

4.5.2 O acesso à internet é concedido aos usuários e colaboradores por meio da identidade digital (*login* e senha) pessoal e intransferível, sendo o titular o único responsável pelas ações e/ou danos, se houver.

4.6 Correio eletrônico

4.6.1 A utilização do correio eletrônico corporativo ou educacional deve se ater à execução das atividades profissionais e educacionais, respeitando as regras de direitos autorais, licenciamento de *software*, direitos de propriedade e privacidade.

4.6.2 O correio eletrônico corporativo ou educacional pode ser utilizado no dispositivo móvel particular, porém o acesso às mensagens e às informações institucionais fora do horário normal de expediente não configura sobrejornada, sobreaviso ou plantão do colaborador, visto que pode ocorrer por ato de liberalidade e/ou conveniência sem a expressa e prévia requisição da instituição.

4.6.3 A utilização de correio eletrônico particular ou público é permitida apenas para a transmissão ou recebimento de conteúdo ou informações particulares, e desde que não lhe seja dada prioridade sobre as atividades profissionais ou acadêmicas, não provoque efeitos negativos para qualquer outro usuário, não viole ou prejudique a rede corporativa e a acadêmica e não viole norma vigente da SMC e suas unidades mantidas.

4.6.3.1 O correio eletrônico particular deverá ser usado somente para interesses particulares do usuário, não podendo ser utilizado para o envio ou recebimento de informações da SMC e suas unidades mantidas.

4.7 Rede sem fio (Wi-Fi)

4.7.1 A SMC e suas unidades mantidas, quando possível, oferecem à comunidade acadêmica e administrativa, nos ambientes autorizados e limitados ao perímetro físico da instituição, uma rede sem fio (Wi-Fi) própria para finalidades educacionais e administrativas.

4.7.2 Somente os alunos e colaboradores expressamente autorizados podem ter acesso à rede sem fio (Wi-Fi) da instituição e devem comprometer-se a fazer uso seguro desse recurso.

4.7.2.1 Em casos excepcionais, visitantes e fornecedores poderão ter acesso à rede sem fio com a prévia autorização do gestor imediato, da GTI ou do CRC.

4.8 Recursos de TIC institucionais

4.8.1 Os recursos de TIC da SMC e das unidades mantidas são destinados a finalidades estritamente profissionais e educacionais, reservadas às atividades e permissões designadas para os usuários.

4.8.2 É vedado o armazenamento de arquivos pessoais nos recursos de TIC da SMC e suas unidades mantidas.

4.8.3 Para a proteção das informações, os arquivos digitais contendo informações da SMC e suas unidades mantidas devem ser armazenados nos servidores de arquivos destinados às áreas e setores específicos, com acesso restrito, considerando que ameaças externas, tais como vírus, interceptação de mensagens eletrônicas e fraudes eletrônicas podem afetar a segurança de tais informações.

4.8.3.1 Os colaboradores devem armazenar os arquivos digitais nos servidores de arquivos específicos e com acesso restrito, disponibilizados na rede corporativa.

4.8.3.2 A GTI e o CRC são responsáveis por realizar as cópias de segurança dos arquivos digitais (*backup*) armazenados nos servidores de arquivos específicos da SMC e suas unidades mantidas.

4.8.3.3 A SMC e suas unidades mantidas não se responsabilizam pelos arquivos digitais armazenados nas estações de trabalho, nos *notebooks*, *tablets* e *smartphones* disponibilizados pela instituição. Em casos de desligamento ou rescisão contratual, os arquivos digitais serão apagados.

4.8.4 Todos os recursos de TIC da SMC e suas unidades mantidas, incluindo os *softwares*, devem ser inventariados e identificados pela GTI.

4.8.5 Só é permitida a utilização de *softwares* e *hardwares* legítimos, previamente homologados ou autorizados pela GTI, sejam eles onerosos, gratuitos, livres ou licenciados.

4.8.6 O desenvolvimento, a manutenção ou definição de aquisição de aplicativos e de sistemas no mercado são de responsabilidade da GTI e do CRC, e precisam atender aos requisitos de segurança em todas as etapas dos processos, a fim de garantir a confidencialidade, integridade, legalidade, autenticidade e disponibilidade das informações.

4.8.7 Todas as modificações nos recursos de TIC da SMC ou das unidades mantidas, principalmente em sistemas e na infraestrutura tecnológica, devem ser realizadas e/ou autorizadas pela GTI ou pelo CRC, e de maneira controlada para identificar os possíveis riscos e prevenir impactos à instituição, além de garantir a disponibilidade dos recursos de TIC e a possibilidade de restauração do ambiente original em caso de incidentes não previstos.

4.8.8 A utilização de recursos deve ser monitorada pela GTI e pelo CRC, aos quais cabe realizar projeções constantes para que os recursos de TIC suportem necessidades tecnológicas futuras.

4.8.9 É vedado o uso de recurso de TIC da SMC e suas unidades mantidas para acessar, baixar, utilizar, armazenar ou divulgar qualquer conteúdo ilícito, impróprio, obsceno, pornográfico, difamatório, discriminatório ou incompatível com o propósito profissional e educacional e as diretrizes da SMC e suas unidades mantidas.

4.8.10 Todo recurso de TIC de propriedade da SMC e suas unidades mantidas, incluindo os dispositivos móveis, devem utilizar recursos de segurança, como senha de bloqueio automático, antivírus, *antispyware*, *firewall* e mecanismos de controle de *softwares* maliciosos.

4.8.11 A retirada de qualquer equipamento, bancos de dados ou *software* das instalações da SMC e suas unidades mantidas, ou da sua infraestrutura tecnológica, deve ser realizada pela GTI e pelo CRC, quando prévia e formalmente autorizada pelo gestor imediato ou por necessidade da GTI ou do CRC.

4.8.12 Dispositivos móveis institucionais

4.8.12.1 O uso de dispositivos móveis de propriedade da SMC ou das unidades mantidas não é permitido por terceiros, prestadores de serviços e visitantes.

4.8.12.2 Os dispositivos móveis institucionais devem conter a menor quantidade possível de informações da SMC e suas unidades mantidas. Arquivos digitais com informações da SMC e suas unidades mantidas, principalmente sobre alunos, devem ser armazenados em servidores específicos para esse fim.

4.8.12.3 Em casos de roubo, perda ou furto do dispositivo móvel institucional que contenha informações da SMC e/ou unidades mantidas, o colaborador deve registrar o Boletim de Ocorrência (B.O.), entregar uma cópia do documento e notificar imediatamente o gestor e a GTI.

4.9 Recursos de TIC particulares

4.9.1 É vedada a conexão dos recursos de TIC particulares na rede corporativa e acadêmica da SMC e suas unidades mantidas.

4.9.1.1 Os docentes são autorizados a utilizar os recursos de TIC particulares, conectados à rede acadêmica, exclusivamente para as suas funções no âmbito educacional, atendendo aos princípios desta Política.

4.9.1.2 A SMC e suas unidades mantidas não têm qualquer responsabilidade sobre a utilização dos *softwares*, arquivos digitais, suporte técnico e manutenções dos recursos de TIC particulares utilizados pelos docentes.

4.9.2 Os recursos de TIC particulares previamente autorizados a acessar os conteúdos e serviços fornecidos pela SMC e suas unidades mantidas devem ser protegidos com uso de métodos de bloqueios de acesso e ferramentas de segurança, como antivírus e *firewall*, a fim de mitigar os riscos de exposição da instituição a ameaças.

4.9.3 Todo recurso de TIC particular trazido para as dependências da SMC ou das unidades mantidas é de inteira responsabilidade de seu proprietário, incluindo os dados e *softwares* nele armazenados ou instalados.

4.9.4 A SMC e suas unidades mantidas não serão responsabilizadas por qualquer perda, furto ou avaria dos recursos de TIC particulares.

4.9.5 Dispositivos móveis particulares

4.9.5.1 O uso de dispositivos móveis particulares é permitido dentro do perímetro físico da SMC e suas unidades mantidas, desde que não interfira nas atividades profissionais e educacionais e esteja de acordo com as leis em vigor.

4.9.5.2 Dentro do perímetro físico e lógico em que informações confidenciais são armazenadas ou processadas, a SMC e/ou unidades mantidas devem restringir a entrada e circulação de dispositivos móveis particulares.

4.9.5.3 Convém que o uso de dispositivos móveis particulares pelos alunos, dentro da sala de aula, seja para finalidades educacionais e didáticas. Caso contrário, o uso deve ocorrer com o prévio conhecimento do docente.

4.10 Armazenamento de informações

4.10.1 Todos devem manter as informações da SMC e suas unidades mantidas armazenadas no local apropriado e destinado a esse fim.

4.10.2 Os colaboradores devem armazenar as informações digitais da SMC e suas unidades mantidas nos servidores da rede corporativa que possuem controle de acesso e cópia de segurança. As informações físicas devem ser guardadas em gavetas, armários trancados ou local apropriado e seguro quando não estiverem sendo utilizadas, principalmente quando envolver, mas não se limitando a, documentação de identificação de aluno, provas ou trabalhos educacionais.

4.10.3 A SMC e/ou unidades mantidas devem solicitar o apagamento e/ou a remoção de conteúdos que estejam nos dispositivos móveis particulares, na internet, nas mídias sociais e/ou em aplicativos, sempre que os mesmos oferecerem riscos aos alunos, colaboradores e à instituição, que forem contrários à legislação nacional vigente, que afetem o bom relacionamento da comunidade acadêmica ou possam configurar algum tipo de dano à instituição.

4.11 Repositórios digitais

4.11.1 Os repositórios digitais para o uso institucional são destinados ao armazenamento, à criação, ao compartilhamento e à transmissão de arquivos (*upload*) de informações da SMC ou de suas unidades mantidas, desde que previamente autorizados, homologados e disponibilizados pela GTI.

4.11.1.1 A utilização dos repositórios digitais para o uso institucional deve estar de acordo com os requisitos de segurança descritos nesta Política.

4.11.1.2 É vedado o armazenamento de arquivos digitais pessoais nos repositórios digitais para uso institucional.

4.11.2 Os repositórios digitais para uso educacional ou acadêmico, objetivando o aprendizado, avaliação ou testes, podem ser utilizados desde que previamente autorizados e homologados pelo CRC.

4.11.3 É vedado armazenar, criar, compartilhar ou transmitir arquivos (*upload*) contendo informações da SMC e suas unidades mantidas para repositórios digitais particulares, principalmente, mas não se limitando a, informações sobre alunos e informações pessoais dos colaboradores.

4.11.4 Em caso de desligamento do colaborador, ou término de contrato de prestação de serviços dos alunos, os arquivos mantidos nos repositórios digitais de uso institucional serão excluídos.

4.11.5 Nos repositórios digitais de uso institucional é vedada a criação, o armazenamento, o compartilhamento e a transmissão de arquivos (*upload*) de informações referentes a qualquer tipo de atividade ilegal, como pornografia infantil, jogos de azar, pirataria, violação dos direitos autorais, marcas comerciais ou outras leis de propriedade intelectual.

4.11.6 É vedado disponibilizar a identidade digital a terceiros para acessar os repositórios digitais de uso institucional.

4.12 Mídias sociais

4.12.1 Os alunos devem adotar um comportamento seguro no acesso e utilização das mídias sociais, em conformidade com todos os direitos e deveres estabelecidos no Regimento Escolar.

4.12.2 A participação institucional do colaborador, por meio de acesso e/ou conexão a mídias sociais a partir do ambiente da instituição e durante o horário de trabalho, deve ser diretamente relacionada à sua função profissional e aos objetivos da SMC e suas unidades mantidas, sendo o colaborador responsável por qualquer ação ou omissão resultante de sua postura e comportamento.

4.13 Mesa limpa e tela limpa

4.13.1 Os papéis contendo informações da SMC e suas unidades mantidas não devem ficar expostos em impressoras, fax, *scanner*, salas de aula, pátios, telas de computadores, áreas comuns, locais de trânsito de pessoas, elevador, refeitório e nas salas de reunião, principalmente quando não estiverem sendo utilizados.

4.13.2 Todos os colaboradores são responsáveis por realizar o bloqueio com senha ao se distanciar do recurso de TIC que estiverem usando, especialmente da sua estação de trabalho ou dispositivo móvel, inclusive quando estiverem em sala de aula.

4.14 Áudio, vídeos e fotos

4.14.1 Não é permitido tirar fotos, gravar, filmar, publicar e/ou compartilhar imagens da SMC e suas unidades mantidas, seja da sala de aula, pátios, corredores, banheiros, vestiários ou qualquer outro local pertencente ao perímetro físico, e também dos alunos e colaboradores, sem prévia autorização.

4.14.1.1 Exceto para situações já previamente avisadas e autorizadas, a exemplo de, mas não se limitando a, eventos educacionais, administrativos, sociais e/ou esportivos, por sua natureza pública e de compartilhamento de informações e desde que o teor do conteúdo não exponha ao ridículo ou gere constrangimento aos envolvidos.

4.14.2 Os alunos dependem de expressa autorização prévia do docente para captar ou reproduzir quaisquer imagens, vídeos ou sons, de dentro da sala de aula, inclusive para o registro por imagem da lousa ou do próprio docente, que devem tão somente ser utilizados para fins pessoais, sendo vedado o seu compartilhamento público, seja pela internet ou por outros meios tecnológicos, bem como a divulgação/reprodução do conteúdo a terceiros não integrantes da instituição.

4.14.2.1 Exceto em situações já previamente avisadas e autorizadas, a exemplo de, mas não se limitando a, eventos educacionais, sociais e/ou esportivos, passeios, excursões e campeonatos.

4.14.3 Os colaboradores da SMC e suas unidades mantidas não devem captar, reproduzir ou compartilhar por meio de qualquer meio tecnológico, inclusive na internet, quaisquer imagens, vídeos ou sons que:

a) Possam comprometer a segurança dos alunos, de outros colaboradores e do ambiente estudantil, acadêmico ou administrativo;

b) Possam comprometer o sigilo das informações; ou

c) Envolvam diretamente a imagem dos alunos, de outros colaboradores, visitantes, prestadores de serviço e fornecedores, sem a prévia e expressa anuência desses ou do gestor responsável, exceto quando autorizados em razão da sua função ou em situações já previamente avisadas e autorizadas a exemplo de, mas não se limitando a, eventos educacionais, sociais e/ou esportivos, passeios, excursões, campeonatos, por sua natureza pública e de compartilhamento de informações.

4.15 Uso de imagem, som da voz e nome

4.15.1 A SMC e suas unidades mantidas podem capturar, guardar, manipular, editar e usar a imagem dos alunos para fins de identificação, autenticação, segurança, registro de atividades, acervo histórico, uso institucional, educativo e social, o que inclui os eventos promovidos pela instituição, inclusive em seus perfis oficiais nas mídias sociais, *website* ou portal acadêmico, intranet, quadro de avisos, revista e/ou jornal universitário ou similar, vídeos educacionais, entre outros conteúdos que possam ser criados ou produzidos em razão da atividade educacional, tendo, por isso, pela própria característica técnica da internet, alcance global e prazo indeterminado, podendo inclusive alcançar *sites* e outros ambientes digitais externos.

4.15.2 Para o uso de imagem, som da voz e nome dos alunos, estão ressalvados os direitos sobre a integridade da sua honra, sua reputação, boa fama ou respeitabilidade, sendo feito apenas nos limites acordados, sem, de forma alguma, expor o aluno ao ridículo ou a situações constrangedoras, atendendo às leis em vigor no Brasil.

4.16 Aplicativos de comunicação

4.16.1 O uso de aplicativos de comunicação no ambiente estudantil ou acadêmico, pelos alunos ou docentes, a partir de recursos institucionais ou particulares, para compartilhar informações acadêmicas, deve ser feito de forma responsável para evitar riscos desnecessários que comprometam atividades, projetos ou a própria instituição.

4.16.2 O uso de aplicativos de comunicação no ambiente de trabalho ou fora dele, pelos colaboradores da SMC e suas unidades mantidas, a partir dos recursos institucionais ou particulares, para compartilhar informações institucionais, deve respeitar sempre o sigilo da informação, atender aos requisitos de segurança previstos nesta Política e respeitar as leis nacionais em vigor para evitar riscos desnecessários relacionados ao vazamento da informação ou que comprometam a instituição.

4.17 Monitoramento

4.17.1 A SMC e suas unidades mantidas realizam o registro e armazenamento de atividades (*logs*) e monitoram seus ambientes físicos e lógicos, com a captura de imagens, áudio ou vídeo, inclusive com a finalidade de proteção de seu patrimônio e reputação, assim como a proteção daqueles com os quais se relacionam de alguma forma.

4.17.2 O armazenamento dos dados monitorados é utilizado para fins administrativos e legais, além de colaborar com as autoridades em caso de investigação.

4.17.3 Em casos de incidentes de segurança e eventos que comprometam a integridade física e lógica dos alunos e colaboradores, a SMC e suas unidades mantidas têm o dever de fornecer informações ao órgão competente para apuração, e quando necessário, disponibilizar provas que estiverem em seu poder ou de cuja existência tiverem conhecimento.

4.18 Combate à intimidação sistemática (*bullying*)

4.18.1 Todos os alunos e colaboradores devem se comprometer a participar de campanhas de conscientização promovidas pela SMC e/ou suas unidades mantidas contra atos de violência e intimidação sistemática, bem como a cooperar de todas as formas em situações críticas para a melhor aplicação de medidas preventivas e reativas, e também contribuir para a apuração de fatos e de pessoas envolvidas em casos de *bullying*, comprometendo-se inclusive a fornecer depoimentos, quando necessários, e provas que estiverem em seu poder ou de cuja existência tiverem conhecimento.

4.19 Contratos de trabalho e de prestação de serviços

4.19.1 O mero porte de dispositivos institucionais e o acesso aos recursos de TIC e/ou às informações institucionais, inclusive de forma remota, fora do horário normal do expediente, em qualquer meio ou canal, incluindo, mas não se limitando a, mensagens de alunos e colaboradores em mídias sociais, mensagens SMS, correio eletrônico institucional, aplicativos e comunicadores instantâneos, por si só, não configuram sobrejornada, sobreaviso ou plantão do colaborador, visto que isso pode ocorrer por ato de liberalidade e/ou conveniência do próprio colaborador sem expressa e prévia requisição da instituição.

4.19.2 Em casos de desligamento, rescisão contratual ou término do contrato, a GTI e o CRC devem desativar todas as identidades digitais do aluno ou colaborador em todos os sistemas e ambientes da SMC e suas unidades mantidas.

4.19.2.1 Nesse caso, o aluno ou colaborador deve excluir todas as informações e contas da SMC e suas unidades mantidas, disponíveis no dispositivo móvel particular, caso tenham sido cadastradas.

4.20 Segurança da informação

4.20.1 Ao repassar ou transmitir informações da SMC e/ou suas unidades mantidas ou sob sua responsabilidade, seja de forma presencial, via telefone, comunicadores instantâneos, mensagens eletrônicas ou mídias sociais, os alunos e colaboradores devem agir com cautela,

confirmando antes a identidade do solicitante e a real necessidade do compartilhamento da informação solicitada.

4.20.2 Os alunos e colaboradores devem ter cautela ao acessar *softwares*, informações e conteúdos disponibilizados gratuitamente na internet, a exemplo de aplicativos, músicas, vídeos, trabalhos completos, livros físicos digitalizados e e-mails com propostas suspeitas, pois podem ser vetores de ataques criminosos.

4.20.3 A GTI e o CRC devem manter um processo de salvaguarda e restauração dos arquivos digitais críticos, a fim de atender aos requisitos operacionais e legais, além de garantir a continuidade do negócio em caso de falhas ou incidentes.

4.20.4 As informações confidenciais, assim como os recursos de TIC que as contenham, quando descartados, devem passar por procedimento de destruição que impossibilite sua recuperação e o acesso às informações armazenadas por pessoas não autorizadas.

4.20.5 Para a proteção das informações e recursos de TIC críticos, a GTI e o CRC devem elaborar um conjunto de estratégias e planos de ação de maneira a garantir que os serviços essenciais sejam devidamente identificados e preservados após a ocorrência de um desastre.

4.20.6 A SMC e suas unidades mantidas estão comprometidas com o dever de orientar constantemente seus alunos e colaboradores no uso seguro das informações e da tecnologia. Por isso, podem realizar programas de educação em segurança da informação para aumentar o nível de cultura em segurança na instituição.

5. PAPÉIS E RESPONSABILIDADES

5.1 Todos

5.1.1 Conhecer e disseminar as regras e princípios da Política de Segurança da Informação.

5.1.2 Preservar e proteger os ativos tangíveis e intangíveis de propriedade ou sob a custódia da SMC e suas unidades mantidas, inclusive todas as suas informações e conteúdos, independentemente do formato ou suporte utilizado, contra todo e qualquer tipo de ameaça, como acesso, compartilhamento ou modificação não autorizados.

5.1.3 Preservar e proteger os recursos institucionais, a marca, a reputação, o conhecimento, a propriedade intelectual da SMC e suas unidades mantidas, principalmente todas as suas informações e conteúdos.

5.1.4 Zelar pela proteção do patrimônio da SMC e suas unidades mantidas, usando com responsabilidade os recursos físicos e lógicos fornecidos;

5.1.5 Evitar a exposição desnecessária das informações, projetos, trabalhos e dependências da SMC e suas unidades mantidas, inclusive nas mídias sociais e na internet, além de agir com responsabilidade no uso dos recursos de TIC e das informações.

5.1.6 Prevenir e/ou reduzir os impactos gerados por incidentes de segurança da informação, garantindo a confidencialidade, integridade, disponibilidade, autenticidade e legalidade das informações.

5.1.7 Cumprir e manter-se atualizado com relação a esta Política, ao Regimento Interno e às demais Normas de Segurança da Informação da SMC e suas unidades mantidas.

5.1.8 Proteger as informações contra acesso, modificação, destruição ou divulgação não autorizados pela SMC e suas unidades mantidas.

5.1.9 Cumprir o dever de combater a intimidação sistemática (*bullying*), por meio da adoção de medidas preventivas e reativas, bem como da conscientização para coibir e conter toda forma de violência dentro da comunidade escolar.

5.1.10 Reportar os incidentes que possam impactar na segurança das informações da SMC e suas unidades mantidas, imediatamente, por meio do endereço incidentes.seguranca@pucminas.br.

5.2 Gestores e coordenadores

5.2.1 Orientar constantemente suas equipes quanto ao uso seguro dos ativos tangíveis e intangíveis, e dos valores adotados pela SMC e suas unidades mantidas, instruindo-as, inclusive, a disseminar a cultura para os demais colaboradores.

5.2.2 Suportar todas as consequências das funções e atividades que delegar a outros colaboradores.

5.2.3 Assegurar o cumprimento desta Política e das demais regulações por parte dos colaboradores supervisionados.

5.2.4 Participar da investigação de incidentes de segurança relacionados às informações, ativos e aos colaboradores sob sua responsabilidade.

5.2.5 Participar, sempre que convocado, das reuniões do Comitê de Segurança da Informação, prestando os esclarecimentos solicitados.

5.3 Colaboradores

5.3.1 Ser cauteloso em relação ao excesso de exposição de sua vida particular, a exemplo de rotinas, trajetos, contatos e intimidades, além do dever de sempre preservar o sigilo profissional nas mídias sociais, a imagem e reputação da instituição e de toda a comunidade escolar (alunos e docentes).

5.3.2 Durante a comunicação, presencial ou digital, com demais colaboradores, alunos, visitantes, fornecedores, prestadores de serviços e outros profissionais, utilizar linguagem respeitosa e adequada, condizente com o ambiente estudantil, acadêmico e administrativo, sem o uso de termos dúbios, com dupla interpretação, que exponham a intimidade ou que denotem excesso de intimidade, abuso de poder, perseguição, discriminação, algum tipo de assédio moral ou sexual.

5.3.3 Utilizar as mídias sociais evitando excessos de exposição e riscos para a sua própria imagem e reputação, bem como para a instituição.

6. DISPOSIÇÕES FINAIS

O presente documento deve ser lido e interpretado sob a égide das leis brasileiras, no idioma português, em conjunto com outras normas e procedimentos aplicáveis pela SMC e suas unidades mantidas.

Quaisquer atitudes ou ações indevidas, ilícitas, não autorizadas ou contrárias ao recomendado por esta Política ou pelas demais normas e procedimentos de segurança da informação da SMC serão consideradas violações por si só e estarão sujeitas às sanções previstas no Regimento Geral, contratos de prestação de serviços, contratos de trabalho e nas demais normas da instituição.

A PSI, bem como as demais normas de segurança da informação da SMC e suas unidades mantidas encontram-se disponíveis no Portal da PUC Minas ou, em caso de indisponibilidade, podem ser solicitadas por meio do endereço seguranca@pucminas.br.

Em caso de dúvidas quanto a esta Política ou aos demais procedimentos de segurança da informação da SMC e suas unidades mantidas, o aluno, docente e colaborador podem solicitar os esclarecimentos necessários pelo e-mail: seguranca@pucminas.br.

Os casos de incidente, infração ou suspeita dessas ocorrências deverão ser comunicados imediatamente, pessoalmente ou por meio do endereço incidentes.seguranca@pucminas.br.

7. DOCUMENTOS DE REFERÊNCIA

O presente documento será complementado pelos Procedimentos, Códigos e Normas de Segurança da Informação da SMC e está em consonância com os seguintes documentos:

- ABNT NBR ISO/IEC 27001:2013 – Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Requisitos;
- ABNT NBR ISO/IEC 27002:2013 – Tecnologia da informação — Técnicas de segurança — Código de prática para controles de segurança da informação;
- ABNT NBR ISO/IEC 27014:2013 – Tecnologia da informação — Técnicas de segurança — Governança de segurança da informação;
- Norma ISO/IEC 27005:2011 – Tecnologia da informação — Técnicas de segurança — Gestão de riscos de segurança da informação;
- COBIT 5® Foundation.

APÊNDICE A – SIGLAS, TERMOS E DEFINIÇÕES

A

Ameaça: Causa potencial de um incidente indesejado, que pode resultar em dano à instituição.

Aplicativos de comunicação: Programas de computador, geralmente instalados em dispositivos móveis, usados para troca rápida de mensagens, conteúdos e informações multimídia, a exemplo de *Whatsapp*, *Telegram* e *Snapchat*.

Ativo: Qualquer coisa que tenha valor para a instituição e precisa ser adequadamente protegida.

Ativos críticos: Todos os recursos considerados essenciais para a instituição que, se não estiverem intactos, disponíveis ou acessíveis, poderão acarretar danos graves à instituição.

Ativo intangível: Todo elemento que possui valor para a instituição e que esteja em meio digital ou se constitua de forma abstrata, mas registrável ou perceptível, a exemplo, mas não se limitando à, reputação, imagem, marca e conhecimento.

Ativo tangível: Bens de propriedade da instituição que são concretos, que podem ser tocados, a exemplo, mas não se limitando a, computadores, imóveis, móveis.

Antivírus: Programa de proteção do computador que detecta e elimina os vírus (programas danosos) nele existentes, assim como impede sua instalação e propagação.

Antispyware: Programa espião de computador que tem o objetivo de observar e roubar informações pessoais do usuário, transmitindo-as para uma fonte externa na internet, sem o conhecimento ou consentimento do usuário.

Autenticidade: Garantia de que as informações sejam procedentes e fidedignas, bem como capazes de gerar evidências não repudiáveis da identificação de quem as criou, editou ou emitiu.

B

Backup: Salvaguarda de sistemas ou arquivos, realizada por meio de reprodução e/ou espelhamento de uma base de arquivos com a finalidade de plena capacidade de recuperação em caso de incidente ou necessidade de retorno.

C

Colaborador: Empregado, estagiário ou menor aprendiz da instituição.

Correio eletrônico: Também denominado e-mail, é um recurso que permite compor, enviar e receber mensagens através de programas eletrônicos de comunicação.

Correio eletrônico corporativo: Destinado a alunos, docentes e colaboradores da instituição, dentro do domínio de cada instituição (Exemplo: joao@pucminas.br).

Correio eletrônico educacional: Destinado a alunos das unidades, dentro do domínio de cada instituição (Exemplo: jose@sga.pucminas.br).

Correio eletrônico particular: Estrutura de correio eletrônico particular não mantido pela instituição (Exemplo: jose@gmail.com).

Confidencialidade: Garantia de que as informações sejam acessadas somente por aqueles expressamente autorizados e sejam devidamente protegidas do conhecimento alheio.

CRC: Centro de Recursos Computacionais, vinculado ao ICEI.

Criptografia: Mecanismo de segurança e privacidade que torna determinada comunicação (textos, imagens, vídeos etc.) ininteligível para quem não tem acesso aos códigos de "tradução" da mensagem.

D

Dados: Conjunto de fatos, valores ou ocorrências em estado bruto, que, quando processados ou agrupados, produzem informações.

Datacenter: Ambiente altamente crítico, projetado para concentrar servidores, equipamentos de processamento e armazenamento de dados, e sistemas de ativos de rede, como *switches*, roteadores e outros.

Disponibilidade: Garantia de que as informações e/ou recursos estejam disponíveis sempre que necessário e mediante a devida autorização para seu acesso ou uso.

Dispositivos móveis: Equipamentos de pequena dimensão que têm como características a capacidade de registro, armazenamento ou processamento de informações, possibilidade de estabelecer conexões e interagir com outros sistemas ou redes, além de serem facilmente

transportados devido à sua portabilidade. Exemplos: *smartphone*, *notebook*, *tablet*, equipamento reprodutor de MP3, câmeras de fotografia ou filmagem.

F

Firewall: Dispositivo de segurança de uma rede de computadores que monitora, autoriza e bloqueia o tráfego que entra e sai da rede.

G

GTI: Gerência de Tecnologia da Informação, vinculada à Diretoria de Infraestrutura da SMC.

I

ICEI: Instituto de Ciências Exatas e Informática da PUC Minas.

Identidade digital: Identificação do usuário em ambientes lógicos, sendo composta por *login* e senha ou por outros mecanismos de identificação e autenticação, como crachá magnético, certificado digital, *token* e biometria.

Incidente de segurança da informação: qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança da informação e levando à perda de um ou mais princípios básicos de confidencialidade, integridade e disponibilidade.

Informação: Conjunto de dados que, processados ou não, pode ser utilizado para produção e transmissão de conhecimento, contido em qualquer meio, suporte ou formato.

Internet: Rede mundial de computadores em que o usuário pode, a partir de um dispositivo, caso tenha acesso e autorização, obter informação de qualquer outro dispositivo também conectado à rede.

Integridade: Garantia de que as informações estejam íntegras durante o seu ciclo de vida.

Intimidação sistemática (*bullying*): Todo ato de violência física ou psicológica, intencional e repetitivo, que ocorre sem motivação evidente, praticado por indivíduo ou grupo, contra uma ou mais pessoas, com o objetivo de intimidá-la(s) ou agredi-la(s), causando dor e angústia à vítima, em uma relação de desequilíbrio de poder entre as partes envolvidas.

L

Legalidade: Garantia de que todas as informações sejam criadas e gerenciadas de acordo com as disposições do ordenamento jurídico em vigor no Brasil.

Login: Nome da identificação única dos usuários para acessarem sistemas computacionais ou recursos tecnológicos.

R

Recursos de tecnologia de informação e comunicação (recursos de TIC): Todos os recursos físicos e lógicos utilizados para criar, armazenar, manusear, transportar, compartilhar e descartar a informação. Exemplos: computadores, *notebooks*, *smartphones*, *tablets*, discos externos, mídias, impressoras, *scanner*, entre outros.

Rede corporativa ou administrativa: Conjunto de recursos de conexão (rede local, rede internet e rede sem fio) para provimento de serviços internos à instituição, disponível para colaboradores, mantida e administrada pela GTI.

Rede acadêmica: Conjunto de recursos de conexão (rede local, rede internet e rede sem fio) para provimento de serviços aos discentes e docentes da instituição. Segregada da rede corporativa, é mantida e administrada pelo CRC.

Repositórios digitais: Coleções de informação digital ou serviços de armazenamento, que podem ser mantidos internamente ou armazenados na internet, a exemplo de, mas não se limitando a, Wikipédia, *Microsoft One Drive*, *Google Drive*, *SkyDrive*, *Dropbox*, *iCloud*.

Risco: Possibilidade de uma ameaça explorar uma vulnerabilidade de um ativo para prejudicar a instituição.

S

Sala de Telecom: Ambiente para armazenar equipamentos de telecomunicações, de conexão e instalações de aterramento e de proteção de rede.

Segurança da informação: Preservação da confidencialidade, integridade e disponibilidade da informação na instituição.

SMS: Sigla de *Short Message Service* (Serviço de Mensagens Curtas). Serviço muito utilizado para o envio de mensagens de textos curtos, através de telefones celulares.

T

TIC: Tecnologia da Informação e Comunicação.

V

Violação: Qualquer atividade que desrespeite as diretrizes estabelecidas na política de segurança da informação ou em quaisquer das demais normas que as complementem.

W

Wi-Fi: Abreviação de *Wireless Fidelity*, que significa fidelidade sem fio, em português. *Wi-fi*, ou *wireless*, é uma tecnologia de comunicação que não faz uso de cabos e, geralmente, é transmitida através de frequências de rádio, infravermelhos etc.