Este documento traz a Política de Privacidade e Segurança da Informação (a “Política”, a “Política de Privacidade e Segurança da Informação”) das CEIs, Centros Universitários e Colégios que compõe as Entidades Camilianas (as “Entidades Camilianas”, a “Empresa”, “nós” ou “nosso/nossa”), de acordo com a Lei Federal n.º 13.709/2018 (a “Lei Geral de Proteção de Dados Pessoais”, a “LGPD”), e que contempla entre as unidades o:

• Centro Educacional São Camilo - Espírito Santo, inscrita no CNPJ sob o nº 58.250.689/0013-26;
• Centro Universitário São Camilo - Espírito Santo, inscrita no CNPJ sob o nº 58.250.689/0007-88;

para informar, orientar e dar ciência sobre as práticas organizacionais de proteção da segurança da informação e promoção da privacidade que regerão os processos e procedimentos específicos adotados pelas unidades de negócios específicas e áreas das Entidades Camilianas.

1. Escopo

Estabelecer as diretrizes e padrões de comportamento desejáveis de colaboradores e prestadores de serviço para proteção da autenticidade, confidencialidade, integridade, acessibilidade responsável, rastreabilidade e privacidade dos ativos de informação das Entidades Camilianas, através da orientação à tomada das melhores práticas técnicas, organizacionais e administrativas mundiais. Dessa forma, evitar danos e prejuízos financeiros, econômicos e reputacionais e mitigar o risco da ocorrência de falhas e incidentes de segurança.

2. Objetivos

As Entidades Camilianas adotam padrões rígidos de ações para:
(a) Assegurar e fomentar a adoção de condutas coerentes com as melhores práticas em privacidade;
(b) Orientar os seus colaboradores à tomada de decisão assertiva e consciente dos valores das Entidades Camilianas;
(c) Assegurar a adoção de medidas de segurança dos ativos de hardware, software e redes e comunicações;
(d) Apoiar, dar suporte, monitorar, acompanhar e avaliar criticamente as medidas de

proteção, detecção, resposta e recuperação dos recursos críticos;
(e) Executar a gestão e avaliar a eficácia das medidas de promoção da Privacidade e Segurança da Informação;
(f) Desenvolver planos de ações de comunicação interna e externa para o mapeamento dos processos que envolvem o tratamento de dados pessoais;
(g) Desenvolver planos de ações de comunicação interna e externa para o mapeamento de riscos à segurança da informação;
(h) Direcionar a implementação de controles operacionais e processos internos para atendimento dos requisitos para promoção da Privacidade e Segurança da Informação.

3. Destinatários

Alunos, Colaboradores e Prestadores de Serviços Internos (individualmente, os "Colaboradores" e os "Prestadores de Serviços Internos", respectivamente, e, quando em conjunto "Todos").

4. Definições

Ativos de Informação. Quaisquer dados, incluindo dados pessoais, hardwares, softwares e outros recursos que possam ser utilizados para o tratamento, tráfego ou armazenamento de informações, aos quais possa ser atribuído valor econômico ou não para as Entidades Camilianas.
Autenticidade. Diretriz da segurança da informação que informa sobre a necessidade de validação da veracidade e legitimidade dos Ativos de Informação.
Colaborador. Pessoa física contratada como funcionário/empregado para trabalhar nas Entidades Camilianas.
Confidencialidade. Garantia de que as informações não são reveladas a quem não detiver o acesso devido e adequado sobre a sua disponibilidade.
Dados pessoais. Espécie de Ativos de Informação protegidos pela Lei Geral de Proteção de Dados Pessoais, relacionada a pessoa natural identificada ou identificável.
Dados sensíveis. Espécie de Dados Pessoais qualificados como sensíveis, de acordo com a Lei Geral de Proteção de Dados Pessoais, relacionados à origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.
Disponibilidade. Garantia de que a informação estará acessível de forma ordenada e precisa quando necessário.
Falha de Segurança. Evento indesejado e/ou inesperado isolado ou em série, acidental

ou causado por terceiro, relacionados à segurança da informação sobre acessos não autorizados, destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito da informação, e que podem comprometer as operações de negócios, ameaçando a segurança da informação.

Incidente de Segurança. Evento indesejado e/ou inesperado isolado ou em série, acidental ou causado por terceiro, relacionados a dados pessoais, sobre acessos não autorizados, destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito da informação, e que podem comprometer as operações de negócios, em ameaça à privacidade dos titulares.

Integridade. Garantia da qualidade, completude, exatidão e precisão das informações.

Prestador de Serviço Interno. Pessoa jurídica contratada para atuar dentro das Entidades Camilianas, sob seu controle e designação de função.

Privacidade. Garantia de que os dados pessoais dos Titulares serão preservados.

Rastreabilidade. Diretriz de Segurança da Informação relativo à possibilidade de rastreio de procedimentos realizados no tratamento de Ativos de Informação.

Recursos de TI. qualquer equipamento de telecomunicações, computação e/ou sistemas ou subsistemas interconectados, utilizados na aquisição, armazenamento, manipulação, processamento, gestão, movimentação, eliminação, controle, exibição, troca, intercâmbio, transmissão, transferência ou recebimento de voz, dados e/ou informações. A definição em questão é intencionalmente ampla, incluindo dispositivos, softwares e serviços conectados a dispositivos ou redes das Entidades Camilianas.

Operação de Tratamento (o "Tratamento"). Toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração

5. Diretrizes Gerais da Política de Privacidade e Segurança da Informação 5.1. Regras Gerais

a) Os Ativos de Informação pertencentes às Entidades Camilianas devem ser operados de forma a preservar a autenticidade, confidencialidade, integridade, rastreabilidade e acessibilidade responsável sobre os seus dados, de forma ética e condizente com as necessidades de manutenção do seu bom uso e controle da exposição a riscos de privacidade e segurança da informação;

b) Os Ativos de Informação devem ser utilizados para cumprir a finalidade legítima e ética para a qual foram operados;
c) Os processos das Entidades Camilianas devem garantir, na medida do possível, a segregação de funções e decisões, através da participação efetiva de mais de um profissional na tomada ou, pelo menos, na revisão de decisões.
d) O acesso aos Ativos de Informação deve ser previsto de forma responsável e documentada, mediante autorização de liberação, conforme necessário para o desempenho das atividades do solicitante;
e) O acesso remoto a Ativos de Informação das Entidades Camilianas em ambiente físico e/ou virtual será realizado de forma a preservar ao máximo a confidencialidade, integridade, acessibilidade e privacidade de dados das Entidades Camilianas e do ambiente acessado, sendo proibida a visualização e/ou tratamento de dados que não sejam necessários à execução das atividades das Entidades Camilianas;
f) Os logins e senhas das Entidades Camilianas são assinaturas eletrônicas e jamais devem ser compartilhadas com terceiros;
g) As responsabilidades de Segurança da Informação poderão ser objeto de comunicação específica para garantir a compreensão dos seus entendimentos e atenção às diretrizes nele estabelecidas;
h) Todo e qualquer relacionamento desenvolvido pelos Colaboradores e Prestadores de Serviços Premium com Terceiros deve ser pautado pelas diretrizes desta Política de Privacidade e Segurança da Informação; e
i) Os Ativos de Informação das Entidades Camilianas devem ser tratados de forma à preservação, manutenção e/ou busca da sua Integridade, Confidencialidade e Acessibilidade responsável.

6. Processos e Procedimentos de Privacidade e Segurança da Informação 6.1 Controle de Acessos

a) Os acessos aos sistemas, relatórios e documentos das Entidades Camilianas são compartilhados de acordo com as necessidades ao desempenho das atividades dos envolvidos; e
b) Na medida do possível, todos os acessos aos Ativos de Informação das Entidades Camilianas serão registrados e rastreáveis, bem como disponibilizados para auditorias.

6.1.1. Criação de Perfil

a) A criação de perfis de acesso deve considerar critérios legítimos de acesso aos ativos

de informação necessários ao desempenho das funções de cada um; e

b) O Gestor responsável pelo Colaborador poderá solicitar a criação de acessos excepcionais, desde que autorizado pela Diretoria da área.

6.1.2. Gerenciamento de Senha

a) Os sistemas das Entidades Camilianas são protegidos por senhas que poderão ser modificadas a qualquer tempo pelo usuário, preferencialmente com autenticação com duplo fator;

b) As senhas são pessoais, confidenciais e intransferíveis;

c) É proibido permitir que outras pessoas que não as titulares do usuário (login) utilizem o sistema em seu nome, seja através do fornecimento ou autorização para uso do login com a senha; e

d) Em caso de suspeita de comprometimento do sigilo das senhas e/ou acesso indevido aos sistemas das Entidades Camilianas por terceiros, todos deverão informar o fato imediatamente ao Data Protection Officer (DPO), através do e-mail dpo@saocamilo.br

6.1.3. Restrição, Revisão e Revogação de Acesso à Informação

a) Qualquer procedimento relacionado à concessão e/ou retirada de acessos deve gerar os registros auditáveis correspondentes.

6.2. Segurança, gerenciamento e controle nas Redes

a) As responsabilidades operacionais pelas redes e pelos recursos computacionais devem estar bem definidas;

b) A confidencialidade e integridade dos dados que trafegam sobre redes sem fio (wireless) devem ser protegidas, bem como os sistemas e as aplicações a conectadas às redes sem fio;

c) Os serviços devem ser gerenciados para assegurar a eficácia dos controles da infraestrutura de processamento dos Ativos de Informação;

d) Os mecanismos implantados para registro e monitoramento de oportunidades de melhorias de detecção, controle e resposta a ações que possam afetar e/ou ser relevantes para a segurança da informação devem ser continuamente avaliados;

e) As atividades de monitoramento devem ser coordenadas de modo a otimizar os serviços e assegurar que os controles sejam aplicados de forma consistente sobre toda a infraestrutura Centro Educacional São Camilo - Espírito Santo e Centro Universitário São Camilo - Espírito Santo;

f) As redes de computadores que suportam os serviços Centro Educacional São Camilo - Espírito Santo e Centro Universitário São Camilo - Espírito Santo devem ser

gerenciadas e controladas para atender as necessidades e o nível de proteção das informações trafegadas, bem como a necessidade de disponibilidade dos seus serviços; e
g) Os controles implementados devem garantir a máxima proteção aos Ativos de Informação.

6.3. Documentos, planilhas e apresentações

a) Documentos de trabalho deverão ser, obrigatoriamente, operados nos sistemas que lhes é devido;
b) Os documentos poderão ser compartilhados de acordo com as regras de utilização de serviços de troca de mensagens e mídias; e
c) É proibido arquivar documentos em pendrives e outros dispositivos móveis.

6.4. Digitalização de documentos

a) A digitalização de documentos deve ser realizada por pessoas previamente autorizadas e que detenham competência e aptidão para realização da tarefa;
b) Documentos digitalizados devem ser assinados digitalmente com certificação digital no padrão ICP-Brasil (Infraestrutura de Chaves Públicas Brasileira) e seguir padrões técnicos mínimos previstos, tais como qualidade da imagem, cores e formatos de armazenamento, além de conter metadados especificados no seu registro;
c) Os documentos digitalizados podem ser descartados após a digitalização, a não ser que sejam documentos históricos, cuja destruição é proibida; e
d) Os documentos digitalizados devem ser protegidos contra alteração, destruição, acesso e reprodução não-autorizados, bem como ter garantida a sua acessibilidade e gerenciamento, a partir da indexação dos metadados registrados.

6.5. Anonimização de Dados Pessoais

a) Sempre que possível, os Dados Pessoais deverão ser anonimizados;
b) O procedimento de anonimização deve garantir a impossibilidade de identificação do Titular de forma irreversível; e
c) As diretrizes e critérios para anonimização de Dados Pessoais deverão ser formalmente apresentadas e registradas em documento específico para tal finalidade determinando os recursos técnicos e administrativos que serão utilizados.

6.6. Manuseio de dados sensíveis

a) Dados pessoais sensíveis devem ter seus mecanismos de segurança da informação reforçados para que não sejam objeto de falha ou incidente de segurança; e
b) Dados pessoais sensíveis poderão ter procedimentos específicos previstos em procedimentos internos para potencializar a garantia da sua confidencialidade,

integridade, acessibilidade, autenticidade e rastreabilidade.

6.7. Transferência de Informação

a) Os Ativos de Informação serão gerenciados e mantidos em redes internas e externas, sendo vedado o acesso não autorizado, duplicação, armazenagem, manipulação, divulgação, transferência, uso ou liberação não aprovada de informações confidenciais das Entidades Camilianas por quem quer que tenha, legítima ou ilegitimamente, acesso a elas;

b) As Entidades Camilianas definirão procedimentos de segurança de transferência e armazenamento de documentos eletrônicos, tais como o uso de repositório de arquivos, mensageiros instantâneos e outras ferramentas adequadas à execução dessas atividades;

c) A agenda dos Colaboradores e Prestadores de Serviços Premium pode ser compartilhada com todos do domínio; e

d) Em qualquer caso, é vedada a transferência de quaisquer comunicados que possam, de alguma forma, ser relacionados a:

• Pornografia, obscenidades e/ou inadequadas para um ambiente profissional;

• Menosprezo, depreciação, incitação ao preconceito de classes, sexo, raça, orientação sexual, idade, religião, política, nacionalidade, deficiência física e/ou qualquer outra que possa desrespeitar alguém;

• Declarações difamatórias, caluniosas e utilização de linguagem ofensiva para ofender alguém;

• Reprodução ilícita de material, que possa infringir direitos autorais, marcas, licenças e patentes;

• Correntes não relacionadas à EMPRESA;

• Uso de e-mail pessoal;

• Divulgação de Ativos da Informação a pessoas não autorizadas.

6.7.1. Trocas de mensagens eletrônicas previamente autorizadas para assuntos profissionais da Diretoria e Colaboradores das Entidades Camilianas

a) E-mail: a ferramenta oficial de e-mail é o Microsoft O365 e todos os colaboradores terão e-mails com terminações @saocamilo-es.br

b) Teams: o colaborador poderá ter o controle e acesso das suas reuniões e poderá criar ou juntar-se a uma reunião. É possível alterar o fundo da sua transmissão para maior conforto no ambiente domiciliar. Caso haja alguma instabilidade no serviço, a ferramenta tem opções de controle de qualidade dos vídeos e áudios, e emite alertas

discretos ao usuário a fim de informá-lo da situação (dê preferência aos fundos oficiais da equipe de Marketing).

c) WhatsApp: É permitido para facilitar a comunicação entre particulares, sendo proibida a troca de dados com Ativos de Informação sobre a unidade, Dados Pessoais, Dados Pessoais Sensíveis, bem como o envio e ecebimento de documentos, seja em DOC, PDF, Foto, anexo, ou qualquer outra forma de divulgação, extração ou difusão. Exceção à proibição é a escolha Centro Educacional São Camilo e Centro Universitário São Camilo - Espírito Santo pelo uso do WhatsApp corporativo em celular corporativo.

d) Essas ferramentas, quando utilizadas em dispositivos corporativos, poderão ser auditadas sempre que necessário à execução de atividades legítimas, com finalidades adequadas e proporcionais à execução das atividades contratadas com as Entidades Camilianas.

6.7.2. Uso de Redes Sociais

a) A utilização das redes sociais deve ser feita com responsabilidade e em nome próprio, não da unidade. Quando a utilização das redes for em nome da unidade, deverão ser observadas as diretrizes da Política específica de Redes Sociais.

6.7.3. Acordos de Confidencialidade

a) Sempre que necessário, as Entidades Camilianas irão firmar acordos de confidencialidade para proteção de Ativos da Informação.

6.8. Medidas Técnicas de Segurança da Informação

6.8.1. A unidade deverá estabelecer os procedimentos técnicos de:

a) Execução de Backup e Restore adequados às necessidades e particularidades do conteúdo protegido e necessidade de disponibilidade e integridade das informações;

b) Instalação dos sistemas e ferramentas de trabalho com feature de segurança adequado e de acordo com o que há de mais atual no mercado;

c) Instruções para tratamento de erros ou outras condições excepcionais que possam ocorrer durante a execução de uma tarefa, incluindo restrições de uso dos utilitários do sistema;

d) Informações para contatos de suporte, caso ocorra eventos operacionais inesperados ou dificuldades técnicas;

e) Procedimentos para o reinício e recuperação, em caso de falha dos Recursos de TI;

f) Gerenciamento de trilhas de auditoria e informações de registros (log) dos Recursos de TI;

g) Proteção contra malwares e softwares maliciosos, tais como firewalls, antivírus e

outras medidas de proteção;
h) Registros e monitoramento de atividades nos sistemas das Entidades Camilianas;
i) Controle de software operacional, tais como inclusão de níveis de acesso para realização de atualizações do sistema operacional, bibliotecas, programas e aplicativos para execução exclusiva de administradores treinados com gerenciamento apropriados, bem como a utilização de softwares legítimos e, em nenhuma circunstância, piratas e/ou ilegais e/ou em desacordo com as normas desta Política de Segurança da Informação;
j) Mesa limpa e tela protegida, mesmo em home office, com a inclusão de mecanismo de travamento de tela por senha quando não estiver em uso; e
k) Acesso remoto através de Virtual Private Network (VPN), com login único e nomeado e devidamente autorizada seguindo o procedimento de solicitação de acesso e controlado via Firewall.

6.8.2. Uso da Internet

a) É proibido utilizar a internet para:
• Prática de qualquer ato ilícito ou fraudulento, incluindo tentativas de acesso não autorizado a sistemas na rede;
• Envio de material ofensivo ou ameaçador para qualquer pessoa e/ou entidade;
• Introduzir qualquer forma de software não autorizado e/ou malicioso na rede;
• Acesso a sites com conteúdo pornográfico;
• Acesso ou download de qualquer material que seja ilegal, ofensivo ou pornográfico; e
• Infringir quaisquer leis e/ou direitos autorais ao navegar na web e ao realizar download de documentos.
b) Todos devem atentar que a identidade das Entidades Camilianas pode ser registrada pelo site visitado e que as Entidades Camilianas poderão manter registro sobre a visitação a qualquer site, o que poderá gerar questionamentos sobre a utilização da internet pela gestão.

6.8.3. Acesso a redes de terceiros

Sempre que possível, dispositivos das Entidades Camilianas e/ou utilizados à prestação de serviços das Entidades Camilianas não devem ser conectados à rede pública (Internet Wi-Fi, modems e circuitos externos) para acesso à internet.

6.8.5. Criptografia

Informações críticas e/ou sensíveis relacionadas a processos internos, informações privadas (dados de funcionários, clientes, terceiros ou fornecedores) ou confidenciais – armazenadas ou circuladas através de dispositivos móveis, ou dos meios de

comunicação das Entidades Camilianas podem ser cifradas, através de métodos criptográficos utilizados pelas Entidades Camilianas.

7. Análise e Gestão de Riscos

Todos são responsáveis pelo mapeamento de processos das suas áreas, bem como pela identificação dos riscos e indicação da probabilidade da ocorrência dos sinistros que podem acontecer sob sua responsabilidade.

7.1. Inventário de Dados Pessoais - elaboração e manutenção da Tabela ROPA

7.1.1. O ROPA

É dever de Todos realizar o mapeamento e o registro de procedimentos de operações realizadas pelas equipes e funcionários, que tratam dados pessoais ("ROPA"), bem como revisar e alimentar este registro, pelo menos uma vez ao ano.

7.1.2. Tabela de classificação de Ativos de Informação

Deve ser elaborado documento de classificação de Ativos de Informação de acordo com a sensibilidade do seu conteúdo e necessidade de proteção da sua segurança, de acordo com as seguintes diretrizes:

(i) Informação confidencial – Dados Pessoais e todas aquelas que versem sobre assuntos que possam ocasionar consequências no âmbito financeiro, legal, reputacional e estratégico para as Entidades Camilianas, seus clientes, Prestadores de Serviços Internos e/ou Colaboradores;

(ii) Informação Pública – informações públicas que podem ser descartadas de forma simples, sem preocupação com o tratamento específico.

7.2. Gestão de Terceiros

7.2.1. Seleção

Os Prestadores de Serviços Internos devem ser avaliados de acordo com requisitos técnicos e organizacionais para avaliação da real disposição de pessoas e recursos necessários à prestação dos serviços e/ou fornecimento dos produtos adequados às exigências de promoção da privacidade e segurança da informação das Entidades Camilianas.

7.2.2. Identificação de Riscos na Contratação

a) As contratações são avaliadas e controladas quanto aos dispositivos contratuais de resguardo dos Ativos da Informação das Entidades Camilianas;

b) É obrigatória a inclusão de cláusula/termo/dispositivo contratual eficaz à mitigação de prejuízos e prevenção de riscos; e

c) Deve ser enviado Manual do Fornecedor das Entidades Camilianas para todos os

fornecedores e Prestadores de Serviços Internos.

7.2.3. Monitoramento e Análise de Prestadores de Serviços Internos que fornecem serviços críticos

Serviços e produtos que possam ser considerados críticos pelo valor interno do relacionamento são monitorados quanto ao desempenho contratual, além das medidas de segurança implantadas para resguardo da segurança da informação.

7.3. Gestão de Falhas e Incidentes de Segurança

Falhas e Incidentes de segurança são eventos adversos, confirmados ou sob suspeita, relacionados à segurança de sistemas de informação e privacidade, que levam à perda de um ou mais princípios básicos desta Política de Segurança da Informação: Confidencialidade, Integridade, Acessibilidade responsável e Privacidade. Nesse caso, o Comitê de Privacidade deverá avaliar a necessidade de acionar o Plano de Gestão de Incidentes e/ou o Plano de Gestão de Continuidade dos Negócios existente nas Entidades Camilianas.

8. Responsabilidades específicas

8.1. Gestores

a) Ter postura exemplar em relação à segurança da informação, servindo como modelo de conduta para os colaboradores sob a sua gestão;

b) Informar, durante as entrevistas de recrutamento de talentos, a necessidade de respeito à Política de Privacidade e Segurança da Informação Interna e as obrigações contratuais em caso de descumprimento; e

c) Estabelecer uma periodicidade para reforço das diretrizes de segurança e promoção da privacidade dentro da sua equipe.

8.2. Corpo Técnico-Administrativo

a) Cumprir as diretivas desta Política e os procedimentos internos definidos pela gestão; e

b) Dominar suas atividades de forma que possa contribuir criticamente com as operações realizadas com os Ativos de Informação das Entidades Camilianas.

8.3. Professores

a) Cumprir as diretivas desta Política e os procedimentos internos definidos pela gestão;

b) Manusear de forma responsável dados sensíveis de alunos; e

c) Jamais compartilhar informações sensíveis e de crianças e adolescentes com outros professores citando o nome de alunos e/ou em desacordo com as determinações contratuais e desta Política.

8.4. Profissionais da Área da Tecnologia

a) Configurar os equipamentos, ferramentas e sistemas concedidos aos colaboradores com todos os controles necessários para cumprir os requerimentos de segurança estabelecidos por esta Política e demais Normas de Segurança da Informação complementares;

b) Os administradores e operadores dos sistemas computacionais podem, pela característica de seus privilégios como usuários, acessar os arquivos e dados de outros usuários. No entanto, isso só será permitido quando for necessário para a execução de atividades operacionais sob sua responsabilidade como, por exemplo, a manutenção de computadores, a realização de cópias de segurança, auditorias ou testes no ambiente;

c) (c) Jamais realizar operações em ambientes de testes, homologação e produção com Dados Pessoais sem a validação do DPO e assinatura de Termo de Confidencialidade competente;

d) Gerar e manter as trilhas para auditoria com nível de detalhe suficiente para rastrear possíveis falhas e fraudes. Para as trilhas geradas e/ou mantidas em meio eletrônico, implantar controles de integridade para torná-las juridicamente válidas como evidências;

e) Administrar, proteger e testar as cópias de segurança dos programas e dados relacionados aos processos críticos e relevantes para as Entidades Camilianas; e (f) Implantar e registar os controles que gerem registros auditáveis para retirada e transporte de mídias das informações custodiadas pela TI, nos ambientes totalmente controlados por ela.

9. Gestão de Consequências

A violação da Política de Privacidade e Segurança da Informação poderá ensejar a punição dos envolvidos, a depender da sua relação com as Entidades Camilianas, sem prejuízo da apuração de perdas e danos judicial e/ou administrativamente e denúncia às autoridades competentes, o que poderá acarretar a responsabilidade penal e civil dos envolvidos, nos termos da legislação aplicável. Internamente, as medidas administrativas serão tomadas conforme segue:

a) Colaboradores: advertência, suspensão, demissão por justa causa;

b) Clientes: aplicação de penalidade contratual, rescisão do contrato; e

c) Prestadores de Serviços (Internos ou não): aplicação de penalidade contratual, rescisão do contrato.

10.Monitoramento Contínuo e Auditoria

A gestão da Área de Tecnologia e o DPO deverão estabelecer rotinas de monitoramento contínuo sobre a eficácia dos controles dispostos nesta Política e auditorias de amostras para avaliação do seu cumprimento.

A Política deverá ser atualizada em periodicidade nunca inferior a anual – ou quando se fizer necessário.

11. Treinamento e Conscientização

As Entidades Camilianas desenvolverão a sua cultura de segurança da informação de acordo com as necessidades e objetivos atuais e futuros da organização. Por isso, em periodicidade nunca inferior a anual, os Destinatários desta Política deverão receber treinamento sobre todos os seus tópicos e outros que se fizerem necessários.

12. Fale conosco!

Se você tiver dúvidas ou conhecer situação que está ou possa estar em desconformidade com esta Política, fale com o nosso Data Protection Officer, o Encarregado da Proteção dos Dados Pessoais dentro da nossa instituição, ele vai dar o tratamento necessário à questão apresentada, com autonomia e independência:

LEE, BROCK E CAMARGO ADVOGADOS (LBCA)

CNPJ: 00.793.310/0001-00

Represenada por: Ricardo Freitas Silveira / Adalberto Fraga Veríssimo Júnior

Contato: dop@saocamilo.br

Controle de Versionamento

Versão1, elaborada em 04/02/2022, aprovada pelo Comitê e DPO e Versão publicada em 27/08/2022

Controle de Mudanças

Versão 2, alterada por DPO e Comitê. Motivo da alteração: ajuste à realidade das unidades. Data 13/06/2024.

Alteraçao dos dados de Encarregado de Dados pessoais em 26.08.2024