skema
BUSINESS SCHOOL

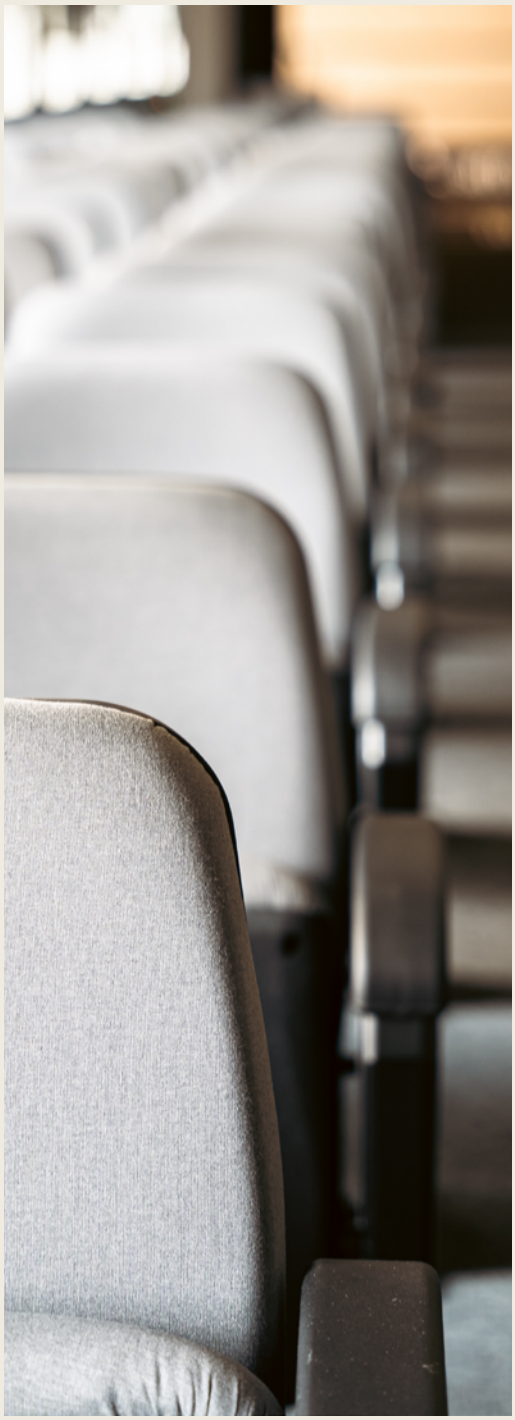
SKEMA BRASIL
POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

2024 | Belo Horizonte, Minas Gerais - Brasil

skema
BUSINESS SCHOOL

Em março de 2015, a SKEMA Business School anunciou a abertura de um novo campus no Brasil em parceria com a Fundação Dom Cabral (FDC).
Assim, a SKEMA tornou-se a primeira e única escola de negócios francesa a oferecer essa experiência na América do Sul, mais especificamente no Brasil, aos seus estudantes.

A SKEMA Business School é uma instituição de educação superior com campi na França, Estados Unidos, China e Brasil, entre outros países. No Brasil, estabeleceu sua presença para oferecer programas de alta qualidade na área de negócios e gestão. Recentemente, expandiu suas atividades para a área da educação jurídica, oferecendo o curso de Direito (bacharelado).



A escolha de Belo Horizonte/MG para a implementação da unidade SKEMA foi motivada pelo fato de ser a terceira cidade mais importante economicamente do Brasil, classificada como um centro de negócios e um parque tecnológico. Isso corrobora com a reputação e identidade das operações da SKEMA Internacional, oferecendo aos seus alunos a oportunidade de estabelecer laços mais estreitos com o mundo dos negócios.

A Instituição tem investido continuamente em metodologias de ensino inovadoras, pesquisa de ponta e parcerias estratégicas com empresas e organizações do setor, proporcionando aos estudantes uma formação completa e alinhada às demandas do mercado de trabalho. Esse compromisso com a qualidade educacional tem se refletido nos resultados obtidos nos indicadores do Ministério da Educação (MEC), consolidando a instituição como uma referência na educação superior, reconhecida tanto nacional quanto internacionalmente.

ÍNDICE

1. INTRODUÇÃO

A informação é um ativo crítico para as empresas e, por esse motivo, precisa ser devidamente protegida. O uso cada vez mais intenso da tecnologia da informação e da interconectividade pelas empresas expõe as informações a ameaças e vulnerabilidades, tornando cada vez mais necessário garantir a sua segurança, integridade, confidencialidade, disponibilidade e autenticidade.

De acordo com a **ABNT NBR ISO/IEC 27002 (2005, p. X)**,

> "seja qual for a forma apresentada ou o meio através do qual a informação é compartilhada e armazenada, é recomendado que ela seja sempre protegida adequadamente."

A presente Política de Segurança da Informação - a PSI - está baseada nas recomendações propostas pela norma **ABNT NBR ISO/IEC 27002:2022, reconhecida mundialmente como um código de prática para a gestão da segurança da informação, bem como está de acordo com as leis vigentes no Brasil.**

Caso os procedimentos estabelecidos no PSI sejam violados, após a apuração dos fatos, a SKEMA reserva-se no direito de aplicar as sanções e medidas disciplinares pertinentes.

2. GLOSSÁRIO

De acordo com o Foundations of Information Security - based on ISO27001 and ISO27002 (4th revised edition), considera-se:

- Dados: são elementos brutos que não possuem significado por si só, mas que podem ser processados e transformados em informação.
- Informação: é um conjunto de dados que ganham sentido e valor quando organizados e interpretados.
- Segurança da informação: é um conjunto de medidas e práticas que visam proteger as informações de ameaças internas e externas, garantindo sua confidencialidade, integridade e disponibilidade.
- Gestão da informação: A gestão da informação descreve o meio pelo qual uma organização planeja, coleta, organiza, utiliza, controla, dissemina e descarta suas informações de forma eficiente, e através da qual garante que o valor dessa informação seja identificado e explorado em toda a sua extensão.
- Política de Segurança da Informação - PSI: é um documento que define as responsabilidades, os procedimentos, as ferramentas e os controles que devem ser adotados para preservar os ativos de informação de uma organização. A PSI deve estar alinhada com os objetivos estratégicos, as necessidades de negócio e as exigências legais e regulatórias da organização. Esta política deve ser revisada periódicamente.
- Ativo de informação: entend-se como um propriedade composta por todos os dados e informações gerados e tratados durante a execução dos sistemas e processos da instituição de ensino.
- Ativo de Processamento: define-se como propriedade composta por todos os elementos de hardware e software necessários para a execução dos sistemas e processos da SKEMA, tanto os produzidos internamente quanto os adquiridos, recebidos por doação ou incorporados.
- Autenticidade: atividade que garante a veracidade da autoria da informação.
- Confidencialidade: somente as pessoas comprovadamente autorizadas devem ter acesso à informação.
- Integridade: os dados só podem sofrer alterações, adições e supressões por pessoas
- Disponibilidade: a informação e os *endpoints* devem estar disponíveis para as pessoas autorizadas sempre que solicitados.

De acordo com o art. 5º incisos I, II, III e X da Lei Federal nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD), considera-se:

I. Dado Pessoal: qualquer informação relacionada à pessoa natural identificada ou

identificável.Documento: unidade de registro de informações, qualquer que seja o suporte ou formato;

II. Titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.

III. Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.

IV. Tratamento: toda operação realizada com dados pessoais, como as que se referem à coleta, à produção, à recepção, à classificação, à utilização, ao acesso, à reprodução, à transmissão, à distribuição, ao processamento, ao arquivamento, ao armazenamento, à eliminação, à avaliação ou ao controle da informação, modificação, comunicação, transferência, difusão ou extração.

V. Consentimento: manifestação livre, informada e inequívoca pela qual o titular ou seu responsável legal concorda com o tratamento de seus dados pessoais para uma finalidade determinada.

VI. Dado Anonimizado: dado relativo ao titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.

VII. Eliminação: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado.

No âmbito da SKEMA ESCOLA DE NEGÓCIOS LTDA, doravante denominada SKEMA, a informação é o dado gerado em contexto envolvido na sua atividade, conforme objeto social, qual seja "desenvolvimento de atividades e administração de instituições nas áreas de educação de nível superior, educação profissional e em outras áreas associadas à educação".

A abrangência da PSI está em todo ambiente da SKEMA, seja ele dentro das dependências da SKEMA ou utilizado de forma remota por seus colaboradores, alunos, professores, gestores e terceirizados

3. OBJETIVO

Definir normas e procedimentos de segurança que visem disciplinar o uso da tecnologia de informação e, consequentemente, garantir a segurança da informação e orientar os colaboradores, professores, alunos, prestadores de serviço e terceirizados quanto à sua importância, conduta e procedimentos adotados pela SKEMA.

Esta política define um conjunto de diretrizes sobre segurança da informação, tendo como referência a ABNT NBR ISO/IEC 27001:2022, a ABNT NBR ISO/IEC 27002:2022 e a legislação brasileira.

A Política de Segurança da Informação visa estabelecer as diretrizes que permitam aos colaboradores, alunos, professores e prestadores de serviço da SKEMA seguirem padrõesde comportamento relacionados à segurança da informação adequados às necessidades de

negócio e de proteção legal da instituição de ensino e do indivíduo.

Sabe-se que a tecnologia da informação é primordial para a realização do objeto social da SKEMA e que os sistemas de computador e os ativos informacionais são acessados dentro e fora das dependências da instituição de ensino.

Nortear a definição de normas e procedimentos específicos de segurança da informação, bem como a implementação de controles e processos para seu atendimento. Preservar as informações da SKEMA BRASIL quanto ao que é denominado como CID – Confidencialidade, Integridade e Disponibilidade, conforme conceituados no Glossário dessa PSI.

4. APLICAÇÃO

Esta Política de Segurança da Informação define diretrizes que devem ser respeitadas e seguidas por alunos, professores, prestadores de serviço, colaboradores e terceirizados que utilizam recursos e tecnologias da infraestrutura física e digital da SKEMA - campus Belo Horizonte, durante suas ações, atividades e tarefas realizadas nos ambientes acadêmicos e administrativos da Instituição.

As diretrizes aqui estabelecidas deverão ser seguidas por todos alunos, professores, prestadores de serviço, colaboradores e terceirizados, e se aplicam à informação em qualquer meio ou suporte. Esta política dá ciência a cada colaborador, aluno, professor, prestador de serviço ou terceiro de que os ambientes, sistemas, computadores e redes da empresa poderão ser monitorados e gravados, com prévia informação, conforme previsto na legislação brasileira.

É também obrigação de cada aluno, professor, prestador de serviço, colaborador e terceirizado se manter atualizado em relação a esta PSI e aos procedimentos e normas relacionadas, buscando orientação da coordenação de ensino do seu gestor ou da Gerência de Tecnologia da Informação sempre que não estiver absolutamente seguro quanto à aquisição, uso e/ou descarte de informações.

5. DISPOSIÇÕES GERAIS

5.1. PRINCÍPIOS

Toda informação produzida ou recebida pelos colaboradores como resultado da atividade profissional contratada pela SKEMA pertence à referida instituição de ensino,

conforme legislação vigente para propriedade intelectual e insdustrial, em especial Lei 9610/98 e Lei 9279/96. As exceções devem ser explícitas e formalizadas em com o Gestor da NSI ou Reitoria, conforme o caso.

Os equipamentos de informática e comunicação, sistemas e informações são utilizados pelos colaboradores para a realização das atividades profissionais. O uso pessoal dos recursos é permitido desde que não prejudique o desempenho dos sistemas e serviços e seja aprovado pelo Gestor da NSI e/ou Reitoria.

A SKEMA, por meio de sua área de Tecnologia da Informação - NSI, poderá registrar todo o uso dos sistemas e serviços de todo e qualquer usuário do ambiente SKEMA, visando garantir a disponibilidade, integridade, confidencialidade e a segurança das informações utilizadas.

A Política da Segurança da Informação ficará disponível para todos nos canais de informação da SKEMA.

5.2. REQUISITOS

Para a uniformidade da informação, a PSI deverá ser comunicada a todos os colaboradores, alunos, professores, prestadores de serviço e terceirizados da SKEMA a fim de que a política seja cumprida dentro e fora da empresa.

Tanto a PSI quanto as normas de privacidade e proteção de dados deverão ser revistas e atualizadas periodicamente e/ou sempre que algum fato relevante ou evento motive sua revisão antecipada, conforme análise e decisão do Comitê de Segurança da Informação.

A responsabilidade em relação à segurança da informação deve ser comunicada na fase de contratação dos colaboradores, alunos, prestadores de serviços e terceirados. Todos os colaboradores devem ser orientados sobre os procedimentos de segurança, bem como o uso correto dos ativos, a fim de reduzir possíveis riscos. Todos os colaboradores, professores, alunos, prestadores de serviço ou terceirizados, devem assinar um termo de responsabilidade. Todo incidente que afete a segurança da informação deverá ser comunicado inicialmente à Gerência de Tecnologia da Informação e ela, se julgar necessário, deverá encaminhar posteriormente ao Comitê Segurança da Informação para avaliação e análise.

Um plano de contingência e a continuidade dos principais sistemas e serviços deverão ser implantados e testados no mínimo anualmente, visando reduzir riscos de perda de confidencialidade, integridade e disponibilidade dos ativos de informação.

Todos os requisitos de segurança da informação, incluindo a necessidade de planos de contingência, devem ser identificados na fase de levantamento de escopo de um projeto ou sistema, e justificados, acordados, documentados, implantados e testados durante a fase de execução.

Deverão ser criados e instituídos controles apropriados, trilhas de auditoria ou

registros de atividades, em todos os pontos e sistemas em que a instituição julgar necessário para reduzir os riscos dos seus ativos de informação como, por exemplo, nas estações de trabalho, notebooks, nos acessos à internet, no correio eletrônico, nos sistemas acadêmicos fornecidos pela SKEMA ou por terceiros.

O não cumprimento dos requisitos previstos nesta PSI e das Normas de Segurança da Informação acarretará violação às regras internas da instituição e sujeitará o usuário às medidas administrativas e legais cabíveis.

5.3. COMITÊ DE SEGURANÇA DA INFORMAÇÃO:

A SKEMA possui um Comitê de Segurança da Informação, bem como Comitê de Privacidade e Proteção de Dados, ambos já instituídos e com reuniões periódicas.

O Comitê de Segurança da Informação é um órgão de natureza consultiva, propositiva e deliberativa, com o intuito de desenvolver políticas internas e planejar ações para difundir e garantir a segurança da informação na SKEMA.

O Comitê de Segurança da Informação, sob coordenação da Gerência de Tecnologia da Informação, é constituído pela Reitoria, Comunicação Institucional e NEAD, tendo como suplentes Jurídico, o Encarregado de Dados e o setor de Recursos Humanos.

A escolha dos membros do Comitê se faz pela Reitoria, devendo ser formalizado por ato interno.

As reuniões do Comitê acontecem, regularmente, uma vez por semana e, em casos especiais, poderão ser agendados outros encontros, considerando as necessidades institucionais.

Sobre as atas das reuniões, o secretário ad hoc será responsável por lavrar os documentos e disponibilizá-los digitalmente para consultas posteriores.

As deliberações, aprovadas pelos membros, serão encaminhadas à Reitoria como sugestões de atos normativos internos.

5.4. RESPONSABILIDADES:

A SKEMA entende que a Política de Segurança da Informação somente será eficaz com o comprometimento de TODOS!

São objetos da PSI os serviços e recursos colocados à disposição dos colaboradores, tais como: computadores, telefones celulares, notebooks, correio eletrônico, Internet (*wi-fi,* e rede cabeada), informações armazenadas em arquivos físicos ou em diretórios da rede, nuvem corporativa e mídias digitais, além de sistemas de aplicação.

As normas descritas no decorrer deste documento devem sofrer alterações sempre

que necessário, sendo que estas devem ser registradas e divulgadas pela empresa, considerando-se o tempo hábil para que eventuais providências sejam tomadas.

Caberá aos responsáveis hierárquicos zelar pelo cumprimento das responsabilidades. Cada colaborador será informado acerca de quem se reportará para fins desta Política.

5.4.1. USUÁRIOS:

- Conhecer, cumprir e fazer cumprir, rigorosamente, o disposto nesta Política de Segurança da Informação;
- Assinar e aderir o Termo de Ciência (BH-SKM-D-021 - TERMO DE CIÊNCIA PSI) para que tenha acesso aos ativos e recursos cedidos pela SKEMA;
- Assumir a responsabilidade pela custódia e segurança das tecnologias computacionais que foram disponibilizadas para fins profissionais;
- Assumir a responsabilidade pelo uso exclusivo e intransferível dos logins e senhas que foram disponibilizadas para fins profissionais;
- Ativar senhas de segurança para o correio eletrônico (e-mail) e sistema operacional, conforme as orientações fornecidas pelo Núcleo de Suporte a Informática (NSI);
- Primar pela busca de conhecimentos e habilidades necessárias para o uso dos softwares e hardwares adequados ao seu contexto de atuação profissional, solicitando a orientação do NSI quando julgar necessário;
- Assegurar medidas básicas de segurança da informação ao realizar atividades profissionais fora das instalações da SKEMA;
- Comunicar ao NSI incidente ou ameaça à segurança da informação e dos recursos computacionais da Instituição;
- Garantir que as informações e os dados pertencentes à SKEMA, clientes e parceiros externos não sejam compartilhados com terceiros nem utilizados para propósitos não autorizados;
- Solicitar ao NSI a compra de licenças e a instalação de softwares que são necessários para suas atividades profissionais, por meio dos canais institucionais;
- Ao término do contrato de trabalho, o usuário deverá entregar as tecnologias fornecidas pela SKEMA (computador, HD, cartão de memória, etc.) e formalizar a devolução por meio do Termo de Responsabilidade de TI;
- Assumir a responsabilidade civil e criminal por quaisquer prejuízos e danos que podem ser provocados em função do descumprimento desta Política de Segurança da Informação.

5.4.2. RESPONSÁVEIS HIERÁRQUICOS

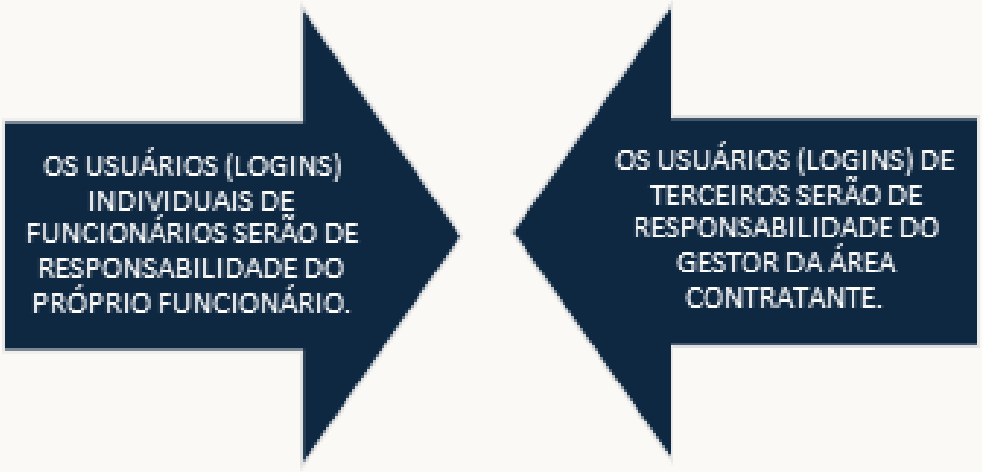
- Apoiar e zelar pelo cumprimento desta PSI, servindo como modelo de conduta para

os colaboradores sob a sua gestão;

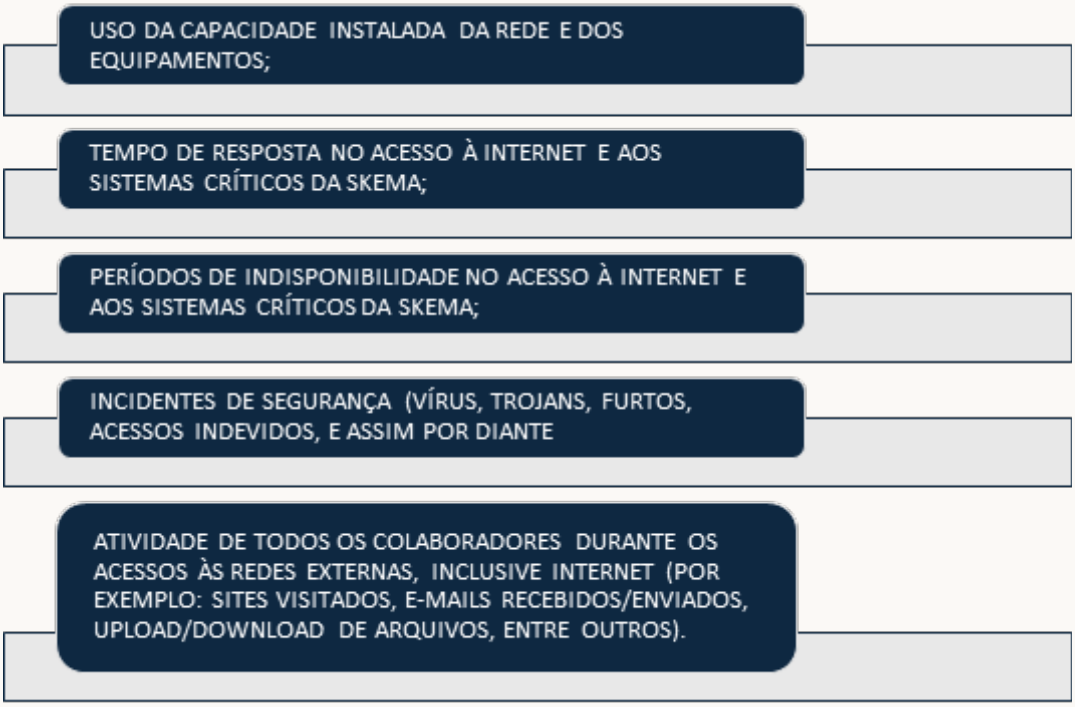
- Exigir a assinatura do Termo de Ciência (BH-SKM-D-021 - TERMO DE CIÊNCIA PSI) dos colaboradores como condição imprescindível para que seja concedido o acesso aos ativos de informação pela instituição;
- Comunicar, durante o processo seletivo de colaboradores, professores e de prestadores de serviços, a importância de se cumprir a PSI da SKEMA.
- Definir o perfil de usuário do colaborador, aluno, professor, prestador de serviço ou terceiro com o NSI para acessar os ambientes virtuais e físicos da SKEMA;
- Informar ao NSI, com antecedência mínima de 03 (três) dias, a data de encerramento do contrato de trabalho do colaborador ou prestador de serviço, para que sejam tomadas as providências institucionais quanto a suspensão do uso das tecnologias da SKEMA para o exercício das atividades profissionais. O RH deverá encaminhar ao NSI o documento **BH-SKM-P-001- PROCEDIMENTO PARA DEMISSÃO DE FUNCIONÁRIOS** devidamente preenchido e assinado;
- Informar ao NSI, com antecedência mínima de 03 (três) dias, promoção ou transferência de área/gerência de colaborador interno, para que sejam realizados os ajustes pertinentes ao novo perfil de usuário e suas permissões de acesso as tecnologias da SKEMA;
- Efetuar revisão periódica dos acessos ao ambiente da SKEMA dos colaboradores do setor, a cada 30 (trinta) dias, validando os perfis atribuidos anteriormente;
- Promover capacitações institucionais, via RH e NSI, quanto ao uso dos recursos computacionais e sistemas de informação;
- Advertir formalmente e aplicar sanções cabíveis ao usuário que violar os princípios ou procedimentos de segurança, relatando imediatamente o fato ao gestor do NSI;
- Obter aprovação técnica do gestor do NSI antes de solicitar a compra de hardware, software ou serviços de informática.
- Orientar os colaboradores quanto à devolução dos recursos colocados à disposição pela SKEMA ao término do contrato de trabalho, nas mesmas condições em que recebeu, assinando a devolução do Termo de Recebimento e Responsabilidade pelos recursos;
- Autorizar o acesso e definir o perfil do usuário junto ao NSI;
- Autorizar as mudanças no perfil do usuário junto ao NSI;
- Orientar os usuários sobre os princípios e procedimentos de Segurança da Informação,
- Notificar imediatamente ao gestor do NSI quaisquer vulnerabilidades e ameaças à quebra de segurança mediante abertura de solicitação no sistema de chamados do NSI;
- Adaptar as normas, os processos, procedimentos e sistemas sob sua responsabilidade para atender a esta PSI.

5.4.3. NÚCLEO DE SUPORTE A INFORMÁTICA (NSI)

- Testar a eficácia dos controles utilizados e informar aos gestores os riscos residuais;
- Acordar com os gestores o nível de serviço que será prestado e os procedimentos de resposta aos incidentes;
- Configurar os equipamentos, ferramentas e sistemas concedidos aos colaboradores com todos os controles necessários para cumprir os requerimentos de segurança estabelecidos por esta PSI e pelas Normas de Segurança da Informação complementares;
- 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;
- Segregar as funções administrativas, operacionais e educacionais a fim de restringir ao mínimo necessário os poderes de cada indivíduo e eliminar, ou ao menos reduzir, a existência de pessoas que possam excluir os logs e trilhas de auditoria das suas próprias ações;
- Garantir segurança especial para sistemas com acesso público, fazendo guarda de evidências que permitam a rastreabilidade para fins de auditoria ou investigação;
- 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;
- Administrar, proteger e testar as cópias de segurança dos programas e dados relacionados aos processos críticos e relevantes para a SKEMA;
- Implantar controles que gerem registros auditáveis para retirada e transporte de mídias das informações custodiadas pela NSI, nos ambientes totalmente controlados por ela;
- O gestor da informação deve ser previamente informado sobre o fim do prazo de retenção, para que tenha a alternativa de alterá-lo antes que a informação seja definitivamente descartada pelo custodiante;
- Quando ocorrer movimentação interna dos ativos de NSI, garantir que as informações de um usuário não serão removidas de forma irrecuperável antes de disponibilizar o ativo para outro usuário;
- Planejar, implantar, fornecer e monitorar a capacidade de armazenagem, processamento e transmissão necessários para garantir a segurança requerida pelas áreas de negócio;
- Atribuir cada conta ou dispositivo de acesso a computadores, sistemas, bases de dados e qualquer outro ativo de informação a um responsável identificável como pessoa física, sendo que:



- Proteger continuamente todos os ativos de informação da empresa contra código malicioso, e garantir que todos os novos ativos só entrem para o ambiente de produção após estarem livres de código malicioso e/ou indesejado;
- Garantir que não sejam introduzidas vulnerabilidades ou fragilidades no ambiente de produção da instituição de ensino em processos de mudança, sendo ideal a auditoria de código e a proteção contratual para controle e responsabilização no caso de uso de terceiros;
- Definir as regras formais para instalação de software e hardware em ambiente de produção da SKEMA, bem como em ambiente exclusivamente educacional, exigindo o seu cumprimento dentro da instituição de ensino;
- Realizar auditorias periódicas de configurações técnicas e análise de riscos;
- Responsabilizar-se pelo uso, manuseio, guarda de assinatura e certificados digitais;
- Garantir, da forma mais rápida possível, com solicitação formal, o bloqueio de acesso de usuários por motivo de desligamento da SKEMA, incidente, investigação ou outra situação que exija medida restritiva para fins de salvaguardar os ativos da instituição de ensino;
- Garantir que todos os servidores, estações e demais dispositivos com acesso à rede da SKEMA operem com o relógio sincronizado com os servidores de tempo oficiais do governo brasileiro;
- Monitorar o ambiente de TI, gerando indicadores e históricos de:



- Propor as metodologias e os processos específicos para a segurança da informação, como avaliação de risco e sistema de classificação da informação;
- Propor e apoiar iniciativas que visem à segurança dos ativos de informação da SKEMA;
- Publicar e promover as versões da PSI e as Normas de Segurança da Informação aprovadas pelo Comitê de Segurança da Informação;
- Promover a conscientização dos colaboradores em relação à relevância da segurança da informação para o negócio da SKEMA, mediante campanhas, palestras, treinamentos e outros meios de endomarketing;
- Apoiar a avaliação e a adequação de controles específicos de segurança da informação para novos sistemas ou serviços;
- Manter comunicação efetiva com o Comitê de Privacidade de Dados sobre assuntos relacionados ao tema que afetem ou tenham potencial para afetar a SKEMA.

5.4. RECURSOS COMPUTACIONAIS

A SKEMA disponibiliza recursos de TI para que seus colaboradores, alunos, prestadores de serviços e terceiros desempenhem, exclusivamente, suas atividades profissionais e acadêmicas.

O colaborador ou terceiro não estão sautorizados a realizarem manutenções,

instalações e modificações na configuração dos equipamentos pré-estabelecida pela equipe de NSI. Além disso, não é permitido a transferência e/ou a divulgação de qualquer software do computador, que possam caracterizar infração de propriedade intelectual.

Ao término do contrato de trabalho ou em situações específicas em que os recursos computacionais não serão mais utilizados pelo colaborador, este deverá encaminhar as tecnologias que estão em sua custódia para que as informações sejam removidas, descartadas ou reutilizadas, de acordo com os processos estabelecidos pelo NSI.

5.5. CONTROLE DE IDENTIFICAÇÃO (LOGIN E SENHA)

A senha é a forma mais convencional de identificação e acesso do usuário, é um recurso pessoal e intransferível que protege a identidade do colaborador, evitando que uma pessoa se faça passar por outra.

O uso de dispositivos e/ou senhas de identificação de outra pessoa constitui crime tipificado no Código Penal Brasileiro (art. 307 – falsa identidade).

Assim, com o objetivo de orientar a criação de senhas seguras, estabelecem-se as seguintes regras:

- A senha é de total responsabilidade do colaborador, aluno, professor, prestador de serviço ou terceiro, sendo expressamente proibida sua divulgação ou empréstimo, devendo a mesma ser imediatamente alterada no caso de suspeita de sua divulgação;
- A senha inicial só será fornecida ao próprio usuário, pessoalmente. Não poderão ser fornecidas por telefone, comunicador instantâneo ou qualquer outra forma que não assegure a identidade do colaborador;
- É proibido o compartilhamento de login para funções de administração de sistemas;
- As senhas não devem ser anotadas e deixadas próximo ao computador (debaixo do teclado, colada no monitor, etc.);
- As senhas deverão seguir os seguintes pré-requisitos:
  a) Tamanho mínimo de dez caracteres;
  b) Existência de caracteres pertencentes a, pelo menos, três dos seguintes grupos: letras maiúsculas, letras minúsculas, números e caracteres especiais;
  c) Não devem ser baseadas em informações pessoais de fácil dedução (aniversário, nome do cônjuge, etc)
- O acesso do usuário deverá ser imediatamente cancelado em situações de desligamento do colaborador ou quando por qualquer razão, cessar a necessidade de acesso do usuário ao sistema ou informação;
- As senhas deverão ser alteradas a cada 90 (noventa) dias.

5.6. USO DE CREDENCIAIS PRIVILEGIADAS

De modo a evitar ataques de invasores em busca de dados sensíveis, aos funcionários da SKEMA será atribuída pela NSI uma conta não-privilegiada dentro da rede da empresa, com exceção a casos especiais de pessoas que obrigatoriamente necessitam de uma conta privilegiada para a realização de suas atividades diárias.

As exceções de acesso privilegiado deverão ter autorização da NSI e/ou da Reitoria.

A gestão das contas de acesso privilegiado é de responsabilidade da NSI, e são as seguintes:

- O controle e atualização das contas de usuário que possuem acesso privilegiado;
- O estabelecimento e aplicação de uma política de gerenciamento de privilégios que determine:
    - o controle das contas e do acesso privilegiado;
    - a criação do inventário e da classificação das contas privilegiadas;
    - aplicação de praticas de segurança e gerenciamento.
- O levantamento e categorização baseada em criticidade dos ativos nas plataformas da organização. Tal levantamente compreende:
    - as paltaformas empregadas (Ex.: plataformas locais, nuvem, Linux, Windows, entre outras.);
    - diretórios e arquivos críticos;
    - hardwares;
    - aplicativos, serviços/daemons, firewalls, roteadores, entre outros.
- O estabelecimento de privilégios mínimos sobre usuários finais, endpoints, contas, aplicativos, serviços, sistemas, etc.;
- A distinção de usuários e processos nos sistemas e redes da instituição, baseando-se em níveis de confiança, necessidades e privilégios;
- O estabelecimento de práticas de segurança para senhas e credenciais;
- O bloqueio de acessos privilegiados no caso de eventuais manutenções à infraestrutura;
- O monitoramento das atividades privilegiadas;
- A implementação de análises de ameaças e de usuários privilegiados.

Os usuários com acesso privilegiado possuem as seguintes responsabilidades:

- A proteção de suas credenciais de acesso privilegiado;
- O consentimento em ter suas atividades monitoradas
- pela NSI para fins de segurança e auditoria;
- O relato a NSI de qualquer atividade suspeita ou não autorizada que tiver ciência;
- A utilização do acesso privilegiado apenas para a realização das atividades profissionais do usuário dentro da organização;

- A preservação do sigilo de dados sensíveis ou confidenciais aos quais tem acesso;
- A preservação dos ativos de informação e equipamentos da organização aos quais tem acesso;
- O cumprimento das políticas e procedimentos de segurança da informação estabelecidos pela organização.

Demais detalhamentos sobre as políticas de gestão e uso de credenciais privilegiadas podem ser consultadas nos documentos **BH-SKM-D-011 - PROCEDIMENTO PARAGESTAO DE CREDENCIAIS – PRIVILEGIOS e BH-SKM-D-019 – USO DE CREDENCIAIS PRIVILEGIADAS.**

5.7. DISPOSITIVOS PESSOAIS

O objetivo da SKEMA é maximizar a agilidade e eficiência da realização das tarefas dos colaboradores, alunos, professores, prestadores de serviços e terceiros, contando com todos os recursos de equipamentos disponíveis.

Excepcionalmente, o NSI ou a Reitoria poderá aprovar que determinados colaboradores, professores ou terceiros possam configurar a conta de e-mail corporativa em seus dispositivos pessoais móveis (em especial, celular), desde que esse dispositivo possua função de encriptação de seu conteúdo. Nesta hipótese, a configuração deve sempre ser realizada pelo NSI.

Ainda, o NSI ou a Reitoria poderá, excepcionalmente, mediante documento expresso e assinado autorizar o uso de equipamentos particulares, desde que se atenda às seguintes condições:

- O NSI deverá verificar as configurações de rede, do aplicativo de antivírus e demais aplicativos instalados para que o acesso à rede interna seja concedido. cumprimento das políticas e procedimentos de segurança da informação estabelecidos pela organização. Aplicativos peer to peer, farejadores de tráfego, softwares que possam gerar carga excessiva na rede, que não estejam de acordo com a legislação vigente ou que possam trazer prejuízos à infraestrutura ou à imagem da SKEMA não serão permitidos. Caso o equipamento não obedeça aos requisitos mínimos de segurança, o acesso não será concedido;
- A SKEMA tem o direito de, periodicamente, auditar os equipamentos utilizados em seu ambiente de rede, visando proteger suas informações bem como garantir que aplicativos ilegais não estejam sendo usados;
- É de responsabilidade do proprietário a instalação do Sistema Operacional que será utilizado, bem como dos aplicativos a serem utilizados no notebook, salvo exceções de aplicativos específicos autorizados pelo NSI;
- É de responsabilidade do proprietário usar somente aplicativos legalizados em seu notebook;
- Não podem ser executados nos notebooks aplicativos de característica maliciosa, que

visam comprometer o funcionamento da rede, acesso a informações sem a devida permissão ou informações confidenciais;

- É proibido o armazenamento de informações que não sejam de uso pessoal do proprietário do notebook. Todos os arquivos que pertençam à SKEMA não podem ser armazenados no disco rígido do notebook ou em dispositivos de armazenamento móvel (ex: pendrive ou HD Externo), sem a autorização da área responsável pelos dados ou pela Reitoria. Estes arquivos devem sempre ser armazenados no servidor de compartilhamento destinado para tal;
- Mesmo nos computadores portáteis fornecidos pela SKEMA, é proibido o armazenamento de informações confidenciais e confidenciais restritas no disco rígido do equipamento.Todo e qualquer software da SKEMA que precise ser instalado em dispositivos pessoais, deverá ser aprovado pelo NSI ou pela Reitoria.

5.8. TELA E MESAS LIMPAS

A padronização da SKEMA para o papel de parede e a proteção de tela de computadores e notebooks deve ser respeitada por todos os colaboradores.

Além disso, é importante que cada um cuide da confidencialidade e privacidade para que papéis, mídias e imagens nos monitores não sejam visualizados por pessoas que não têm acesso autorizado pela Instituição.

Neste sentido, o colaborador também deverá bloquear o computador quando não estiver utilizando o equipamento. Após 5 (cinco) minutos em que o computador estiver em stand-by, a sessão será finalizada. Ao reiniciar as atividades, será solicitado o login e senha para que o usuário reestabeleça o acesso.

5.9. MÍDIAS REMOVÍVEIS, PORTAS USB E BLUETOOTH

Mídias removíveis são dispositivos que permitem a leitura e gravação de dados tais como: CD, DVD, Pen Drive, cartão de memória, HDs portáteis, telefones celulares, entre outros. A porta USB é o principal ponto de vulnerabilidade de segurança, podendo ser usada para a fuga de informações corporativas confidenciais.

Tal vulnerabilidade não pode ser contida com firewalls já que os dispositivos são acoplados aos equipamentos pelos próprios funcionários da empresa. Para minimizar os riscos de exposição e perda de dados sensíveis mantidos pela empresa e reduzir os riscos de proliferação de malwares nos computadores, a transferência de informações para dispositivos removíveis é bloqueada nos equipamentos da empresa.

Com o objetivo de prevenir a disseminação de malwares nos computadores da Instituição, o uso de dispositivos removíveis será permitido apenas para funcionários autorizados. Esses funcionários serão identificados por meio de seus nomes de usuário ao

acessarem o sistema, diferenciando-os de outros usuários. As portas USB e a funcionalidade Bluetooth estarão desativadas para usuários não autorizados.

Nesse contexto, se um usuário não autorizado tentar utilizar uma mídia removível, receberá uma mensagem do sistema explicando o motivo da falha na leitura do dispositivo. Adicionalmente, todas as mídias removíveis, incluindo as de usuários autorizados, passarão por uma verificação do antivírus assim que forem conectadas ao computador. A leitura do dispositivo será bloqueada caso seja detectado qualquer malware.

A liberação das portas USB dos desktops e notebooks é feita somente se o uso for justificado e aprovado expressamente pelo NSI e/ou Reitoria. O dispositivo USB deve ser preferencialmente adquirido pela empresa, está criptografado e protegido por senha. O dispositivo só é liberado para utilização na sua diretoria. Mesmo em equipamentos liberados o tráfego de dados entre as unidades USB e os computadores é monitorado através relatórios providos pelo sistema de gerenciamento, auditorias internas e externas, e validações feitas pelo comitê de segurança da informação e compliance.

5.10. DESCARTE DE MÍDIAS

Quando houver necessidade de descarte de mídias, o colaborador deverá destruir a tecnologia que armazena e transmite as informações. Compreende-se como mídia CD, DVD, papel, pen drive, HD externo, entre outros.

Para isso, é fundamental que esse processo de eliminação siga as orientações contidas nos documentos BH-SKM-D-020 - **INSTRUÇÕES NORMATIVAS DE RETENÇÃO E DESCARTE DE DADOS e BH-SKM-D-016- INSTRUÇÕES NORMATIVAS DE DESCARTE DE EQUIPAMENTOS ELTROELETRONICOS – Rev3.**

O obejtivo é evitar que as mídias sejam recuperadas e, com isso, as informações de propriedade da SKEMA ou controladas pela empresa sejam utilizadas por terceiros.

Caberá ao NSI avaliar se há necessidade de descarte da mídia ou se será possível o reaproveitamento apenas da tecnologia para uso posterior na SKEMA.

O NSI promoverá o descarte das mídias dentro das normas de segurança da informação.

5.11. CLASSIFICAÇÃO DA INFORMAÇÃO

Os gestores da SKEMA serão responsáveis em difundir a classificação dos documentos abaixo mencionados. Caso o gestor tenha dúvidas com a classificação da informação contendo dados pessoais, deverá solicitar auxílio do encarregado de dados (DPO).

Todas as informações circulantes interna e externamente originadas pela SKEMA BUSINESS SCHOOL , devem ser classificadas por rótulos considerando Pública, Interna, Confidencial e Restrita conforme descrição a seguir:

PÚBLICA: Refere-se às informações explicitamente aprovadas por seu responsável para consulta irrestrita e cuja divulgação externa não comprometam as atividades da SKEMA e que, por isso, não necessitam de proteção efetiva ou tratamento específico. São exemplos de informação pública:

a) Informações acadêmicas;

b) Rotinas e agendas de aulas;

c) Campanhas de conscientização para alunos, professores e colaboradores.

INTERNA: Refere-se às informações disponíveis aos colaboradores da SKEMA para a execução de suas tarefas rotineiras, não se destinando, portanto, ao uso do público externo. São exemplos de informações internas:

a) Memorandos, Portarias, Padrões, Políticas e Procedimentos internos;

b) E-mails e lista telefônica internos;

c) Avisos e campanhas internas;

CONFIDENCIAL: Refere-se às informações de acesso restrito a um colaborador ou grupo de colaboradores. Sua revelação pode violar a privacidade de indivíduos, violar acordos de confidencialidade, dentre outros. São exemplos de informações confidenciais:

a) Exames médicos e dados pessoais sensíveis dos colaboradores;

b) Processos judiciais;

c) Dados cadastrais de funcionários.

RESTRITA: Refere-se às informações de acesso restrito a um colaborador ou grupo de colaboradores que obrigatoriamente contam como destinatários da mesma, em geral, associadas ao interesse estratégico da empresa e restritas ao superintende, gerentes e funcionários cujas funções requeiram conhecê-las. São exemplos de informações confidenciais restritas:

a) Atas de reunião da governança com a diretoria da SKEMA;

b) Indicadores e estatísticas financeiras da SKEMA;

5.11.1. SIGILO E CONFIDENCIALIDADE

Toda informação disponibilizada ou coletada pelo colaborador, em razão do desempenho de suas funções e atividades, é de propriedade da SKEMA, classificada como confidencial, tendo seu uso restrito às suas atividades, incluindo-se, dentre outras, todas e quaisquer informações orais e/ou escritas, transmitidas e/ou divulgadas pela empresa.

Informação confidencial significa, sem se limitar a, toda e qualquer informação de qualquer natureza - técnica, operacional, comercial e jurídica -, incluídas em descrição ou documentos que envolvam o know-how da empresa, planos de negócios, métodos de contabilidade, técnicas e experiências acumuladas, documentos técnicos e administrativos, contratos, papéis, estudos, pareceres, pesquisas, transmitidas pela empresa ao (a) colaborador (a) ou por ele (a) coletada.

- O colaborador concorda em usar as informações confidenciais recebidas da empresa com o propósito restrito de se fazer cumprir o estabelecido e acordado no contrato de trabalho.
- O colaborador que receber informação confidencial somente poderá usá-la para o propósito estabelecido no item anterior, e zelará para que tal informação confidencial não seja, de qualquer forma, divulgada ou revelada a terceiros.
- Exceto quando imprescindíveis ao desenvolvimento das ações da SKEMA e integre as suas atividades, não será permitido ao colaborador que receberá informação confidencial, produzir cópias ou backup, por qualquer meio ou forma, de qualquer um dos documentos a ele fornecidos ou documentos que tenham chegado a seu conhecimento em virtude do contrato, considerando que todas sejam informações confidenciais.
- Quando fornecida ou revelada por outras pessoas ou clientes, toda informação permanecerá sendo de sua propriedade, somente podendo ser usada pela SKEMA ou pelos colaboradores para os fins de execução do contrato. Tais informações confidenciais, incluídas as cópias realizadas, serão retornadas às pessoas e clientes, ou então destruídas pela empresa, tão logo tenha terminado a necessidade de seu uso ou tenha sido solicitado por eles e, em qualquer caso, na hipótese de término da vigência do contrato, observados as condições nele estabelecidas
- O colaborador que receber informação confidencial se obriga a:

I. Não discutir perante terceiros ou quaisquer colaboradores que não a recebeu anteriormente, usar, divulgar, revelar, ceder a qualquer título ou dispor dessas informações, para nenhuma pessoa, física ou jurídica, e para nenhuma outra finalidade que não seja exclusivamente relacionada ao objeto referido, cumprindo-lhe adotar cautelas e precauções adequadas no sentido de impedir o seu uso indevido por qualquer pessoa que, por qualquer razão, tenha tido acesso a elas.

II. Responsabilizar-se por impedir, por qualquer meio em direito

admitido, a divulgação ou a utilização de informações.

III. Restituir imediatamente o documento (ou outro suporte/mídia) que contiver as informações confidenciais às pessoas ou clientes, sempre que este as solicitar ou sempre que estas deixarem de ser necessárias, e não guardar para si, em nenhuma hipótese, cópia, reprodução ou segunda via das mesmas.

- Fica ciente o colaborador que receber informação confidencial que as obrigações de confidencialidade, tanto quanto as outras responsabilidades e obrigações, vigorarão durante e após todo o contrato de trabalho, mesmo após o seu desligamento da empresa.
- O colaborador que recebe e tem conhecimento de informação confidencial, reconhece e aceita que, na hipótese de violação de quaisquer dos tópicos mencionados acima, estará sujeito (a) as sanções e penalidades legais, em especial a prevista no art. 482, da Consolidação das Leis do Trabalho, que trata da rescisão do contrato de trabalho por justa causa, sem prejuízo das perdas e danos que der causa, estas estimadas pela empresa, inclusive as de ordem moral ou concorrencial, bem como as de responsabilidades civis e criminais respectivas.

5.11.1. SIGILO E CONFIDENCIALIDADE

Sempre que Informações Protegidas forem transmitidas por meio de comunicação verbal, o colaborador deverá respeitar as regras dispostas abaixo, de acordo com o meio de transferência da informação:

(i) Presencial. Informações Internas, Confidenciais e Secretas somente podem ser discutidas em locais privados de acesso controlado, para impedir que terceiros não autorizados escutem a conversa e tenham acesso a tais informações. Quando não for possível trocar tais informações em ambiente privado, o colaborador deverá tomar, no mínimo, as seguintes cautelas:

(a) sempre verificar se alguém está escutando a conversa; e

(b) nunca identificar a SKEMA durante o diálogo.

(ii) Telefones, Celulares, Smartphones e Rádios. É vedada a transmissão de informações confidenciais e secretas por rádio ou telefone (fixo ou móvel). Caso o colaborador não possa evitar que tais informações sejam transmitidas por ligações telefônicas ou outros meios de transmissão, o colaborador deve redobrar o cuidado, sendo objetivo e discreto ao transmitir tais informações. Da mesma forma, o colaborador também não deve fornecer informações como senhas, telefones, endereços (físicos e eletrônicos), informações pessoais ou outros dados de acessos restrito por telefone ou outros meios de transmissão e deve estar atento para não repetir em voz alta essas informações quando forem lhe passar por terceiros. Ainda, o colaborador entende e concorda que é vedada a gravação de Informações Confidenciais e Secretas em equipamentos eletrônicos, como caixa postal, secretária eletrônica, áudios no

WhatsApp ou aplicativos similares.

(iii) VOIP. Os colaboradores que tiverem acesso autorizado à ferramenta de VOIP devem se atentar às mesmas regras do uso de telefones, celulares e rádio de comunicação. Ainda, devem estar cientes que tal ferramenta é de titularidade exclusiva da SKEMA, podendo somente ser utilizada para realização das atividades relacionadas aos negócios e interesse da SKEMA.

5.12. PROTEÇÃO: ANTIVÍRUS

Todos os computadores e telefones corporativos da SKEMA possuem antivírus instalados. Assim que é lançada uma nova versão do software, é iniciada uma atualização automática por meio do aplicativo servidor.

A fim de garantir a segurança, o NSI alerta que é proibido a remoção ou alteração nas configurações do antivírus.

O software executará verificações automatizadas no discorígido (HD/SSD) dos computadores, conforme configurações pré-definidas para a execução periódica do antivírus na estação de trabalho.

Além disso, sempre que uma mídia externa for utilizada, seja via USB ou entradas para cartões, um escaneamento dos arquivos será iniciado imediatamente ao serem conectados ao computador institucional.

As checagens do disco rígido (HD/SSD) da estação de trabalho estão programadas para execução periódica automática, conforme definições do NSI.

É importante a instalação de antivírus nos telefones corporativos, a fim de garantir segurança das informações acessadas nos dispositivos.

Nos casos em que é permitido ao usuário o uso de mídias externas, como pendrives e HDs, são programados escaneamentos assim que for conectado ao computador.

5.13. E-MAIL CORPORATIVO

O objetivo desta norma é informar aos colaboradores da SKEMA quais são as atividades permitidas e proibidas quanto ao uso do correio eletrônico corporativo (usuario@skema.edu).

O uso do correio eletrônico da SKEMA é para fins corporativos e relacionados às atividades do colaborador usuário dentro da instituição. A utilização desse serviço para fins pessoais é permitida desde que feita com bom senso, não prejudique a SKEMA e também não cause impacto no tráfego da rede.

Acrescentamos que é proibido aos colaboradores o uso do correio eletrônico da SKEMA:

- enviar mensagens não solicitadas para múltiplos destinatários, exceto se relacionadas a uso legítimo da instituição;
- enviar mensagem por correio eletrônico pelo endereço de seu departamento ou usando o nome de usuário de outra pessoa ou endereço de correio eletrônico que não esteja autorizado a utilizar;
- enviar qualquer mensagem por meios eletrônicos que torne seu remetente e/ou a SKEMA vulneráveis a ações civis ou criminais;
- divulgar informações não autorizadas ou imagens de tela, sistemas, documentos e afins sem autorização expressa e formal concedida pelo proprietário desse ativo de informação;
- falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários, com o objetivo de evitar as punições prevista;
- apagar mensagens pertinentes de correio eletrônico quando em qualquer eventualidade a SKEMA estiver sujeita a algum tipo de investigação;

Produzir, transmitir ou divulgar mensagem que:

- contenha qualquer ato ou forneça orientação que conflite ou contrarie os interesses da SKEMA;
- contenha ameaças eletrônicas, como: spam, mail bombing, vírus de computador;
- contenha arquivos com código executável (.exe, .com, .bat, .pif, .js, .vbs, .hta, .src, cpl, .reg, .dll, .inf) ou qualquer outra extensão que represente um risco à segurança;
- vise obter acesso não autorizado a outro computador, servidor ou rede;
- vise interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;
- vise burlar qualquer sistema de segurança;
- vise vigiar secretamente ou assediar outro usuário;
- vise acessar informações confidenciais sem explícita autorização do proprietário;
- vise acessar indevidamente informações que possam causar prejuízos a qualquer pessoa;
- inclua imagens criptografadas ou de qualquer forma mascaradas;
- tenha conteúdo considerado impróprio, obsceno ou ilegal;
- seja de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico entre outros;
- contenha perseguição preconceituosa baseada em sexo, raça, incapacidade física ou mental ou outras situações protegidas;
- tenha fins políticos locais ou do país (propaganda política);
- inclua material protegido por direitos autorais sem a permissão do detentor dos

direitos.

As mensagens de correio eletrônico sempre deverão incluir assinatura com o seguinte formato:

- Nome do colaborador;
- Gerência ou departamento;
- Nome da empresa;
- Telefone(s);
- Correio eletrônico;
- Classificação da informação conforme descrito nesta PSI.

5.14. A REDE DA SKEMA

5.14.1. DIREITO DE USO

A rede SKEMA e os equipamentos que a compõem podem ser utilizadas pelos usuários cadastrados institucionalmente para que exerçam suas atividades profissionais, durante o horário de expediente da empresa.

Os usuários cadastrados que tem direito de uso da rede são: funcionários, diretores, prestadores de serviços terceirizados, entre outros.

Para o uso da internet, acesso à rede e criação de e-mail corporativo (usuário@skema.edu), serão previamente autorizados pela SKEMA, ou por seus representantes através de comunicação ao NSI por meio de chamado.

O direito de uso da rede cessa quando o usuário encerrar seu vínculo regular com

a SKEMA, seja através do desligamento por qualquer motivo, suspensão do contrato de trabalho ou serviço prestado ou pelo encerramento de atividades que justifiquem seu acesso à rede.

5.14.2. RESPONSABILIDADES INDIVIDUAIS

O usuário tem as seguintes responsabilidades na segurança e sigilo da rede da SKEMA:

a. Zelar pela rede e pelos equipamentos que utiliza, não sendo permitida qualquer remoção, desconexão de partes, substituição, reconfiguração ou qualquer alteração nas características físicas ou técnicas dos equipamentos integrantes da rede;

b. Estar ciente de que o login de acesso ou senha à rede é pessoal e intransferível, devendo, portanto, proceder de forma responsável, garantindo o sigilo de sua senha, trocando-os de acordo com as orientações da SKEMA e escolhendo códigos de difícil decodificação;

c. Respeitar áreas de acesso restrito, não executando tentativas de acesso a áreas e/ou equipamentos alheios as suas permissões de acesso;

d. Não tomar atitude ou ação que possa, direta ou indiretamente, danificar ou indisponibilizar recursos da rede por qualquer intervalo de tempo;

e. Não executar programas que tenham como finalidade a decodificação de senhas, a monitoramento da rede, a leitura de dados de terceiros, a propagação de vírus de computador, a destruição parcial ou total de arquivos ou a indisponibilização de serviços;

f. Não instalar ou executar programas, instalar equipamentos ou executar ações que não sejam previamente autorizados pela SKEMA ou que possam facilitar o acesso à rede de usuários não autorizados;

g. Não fazer uso de direitos especiais de acesso ou de qualquer outro privilégio já extintos com o término do período de ocupação de cargo ou função dentro da SKEMA;

h. Utilizar a rede corporativa de maneira profissional, ética, segura e legal, mesmo em horários de intervalo e fora do horário de trabalho;

i. Em caso de dúvidas em relação à utilização e segurança da rede, contatar previamente ao NSI através de e-mail ou outros meios de comunicação que venham a ser oferecidos, e seguir suas orientações.

5.15. DISPOSITIVOS MÓVEIS

A SKEMA deseja facilitar a mobilidade e o fluxo de informação entre seus colaboradores regulamentando o uso de equipamentos portáteis.

Quando se descreve “dispositivo móvel” entende-se qualquer equipamento eletrônico com atribuições de mobilidade de propriedade da instituição, ou aprovado e permitido pelo NSI e/ou Reitoria, como: notebooks, smartphones, pendrives e HDs externos.

Essa norma visa estabelecer critérios de manuseio, prevenção e responsabilidade sobre o uso de dispositivos móveis e deverá ser aplicada a todos os colaboradores que utilizem tais equipamentos.

A SKEMA, na qualidade de proprietária dos equipamentos fornecidos, reserva-se o direito de inspecioná-los a qualquer tempo, caso seja necessário realizar uma manutenção de segurança.

O colaborador, portanto, assume o compromisso de não utilizar, revelar ou divulgar a terceiros, de modo algum, direta ou indiretamente, em proveito próprio ou de terceiros, qualquer informação, confidencial ou não, que tenha ou venha a ter conhecimento em razão de suas funções na SKEMA, mesmo depois de terminado o vínculo contratual mantido com a instituição.

O suporte técnico aos dispositivos móveis de propriedade da SKEMA e aos seus usuários deverá seguir o mesmo fluxo de suporte contratado pela instituição.

Todo colaborador, professor, prestador de serviço ou terceiro deverá utilizar senhas de bloqueio automático para seu dispositivo móvel. Não será permitida, em nenhuma hipótese, a alteração da configuração dos sistemas operacionais dos equipamentos, em especial os referentes à segurança e à geração de logs, sem a devida comunicação e a autorização da área responsável e sem a condução, auxílio ou presença de um técnico do NSI.

O colaborador deverá responsabilizar-se em não manter ou utilizar quaisquer programas e/ou aplicativos que não tenham sido instalados ou autorizados por um técnico do NSI.

A reprodução não autorizada dos softwares instalados nos dispositivos móveis fornecidos pela instituição constituirá uso indevido do equipamento e infração legal aos direitos autorais do fabricante.

É permitido o uso de rede banda larga de locais conhecidos pelo colaborador como: sua casa, hotéis, fornecedores e alunos.

É responsabilidade do colaborador, no caso de furto ou roubo de um dispositivo móvel fornecido pela SKEMA, notificar imediatamente seu gestor direto e o NSI.

Também deverá procurar a ajuda das autoridades policiais registrando, assim que possível, um boletim de ocorrência (BO).

O colaborador deverá estar ciente de que o uso indevido do dispositivo móvel caracterizará a assunção de todos os riscos da sua má utilização, sendo o único responsável por quaisquer danos, diretos ou indiretos, presentes ou futuros, que venha causar à SKEMA e/ou terceiros.

5.16. HOME OFFICE

O colaborador que estiver sob a condição de home office, terá as seguintes formas de executar suas tarefas e funções longe da sede da SKEMA:

1. Utilizar equipamento de propriedade da Instituição, que será levado para o domicílio do colaborador, ficando, assim, sob seus cuidados e responsabilidade;
2. Utilizar equipamento particular para acesso remoto ao computador da instituição ou aos dados armazenados em nuvem.

A decisão sobre qual dos dois métodos será utilizado pelo colaborador deve ser feita em conjunto com o gestor, para assim selecionar a opção mais adequada para a execução do trabalho.

A forma ou o método de acesso às informações no ambiente virtual e físico da SKEMA será definida pela NSI.

Em qualquer das situações, o colaborador se compromete a proteger a integridade dos equipamentos e dados da instituição, utilizando mecanismos de segurança como sistemas de criptografia, antivírus e Redes Privadas Virtuais (VPNs), conforme mencionado anteriormente nesta política.

5.17. UTILIZAÇÃO DE IMPRESSORAS E OUTROS RECURSOS

O uso de impressoras na SKEMA BUSINESS SCHOOL deve seguir algumas regras:

- É proibida a impressão e xerox de documentos de cunho pessoal e/ou ilegal;
- A configuração e manutenção das impressoras só podem ser realizadas pela equipe técnica do NSI e/ou profissionais designados por eles;
- O responsável de cada departamento, será o responsável pelas impressões realizadas em seu departamento, inclusive para responder a questionamentos relacionados ao excesso de impressão;
- Toda impressão realizada, deve ser imediatamente coletada pelo usuário, sendo terminantemente proibido a permanência junto à bandeja da impressora após o expediente de trabalho, podendo o usuário responder por violação à esta PSI.
- Todas as impressões e cópias efetuadas pelas impressoras da SKEMA só poderão ser realizadas mediante o uso de senhas previamente cadastradas pelo NSI, evitando que as informações fiquem expostas sobre os gaveteiros das impressoras ou mobiliário. As impressões que permanecerem nas impressoras, gaveteiro ou mobiliário próximo serão descartadas por via do triturador de papel.

5.18. ADIÇÃO DE RECURSOS/EQUIPAMENTOS À REDE SKEMA

Para adicionar novos equipamentos na rede, o colaborador deve solicitar ao NSI para aprovação institucional.

Após a autorização o equipamento será integrado à rede, obedecendo os processos e padrões de instalação, de utilização e de designação de endereços e domínio estabelecidos pela NSI.

Somente recursos adicionados pelo NSI estarão em conformidade com as diretrizes de segurança da rede, potencializando assim a administração e a assistência do equipamento em conformidade com a qualidade tecnológica delineada pela SKEMA.

5.19. ARMAZENAMENTO DE ARQUIVOS DE TRABALHO

Todos os arquivos contidos nos servidores de rede e no Sharepoint devem ser exclusivamente de interesse da SKEMA. É proibida a criação de pastas pessoais nos servidores da rede.

Todos os arquivos produzidos pelos colaboradores para os serviços da SKEMA devem ser salvos no Sharepoint do usuário (One Drive) ou no site adequado do setor.

Cada setor possui seu próprio diretório, tendo acesso limitado apenas para os colaboradores de suas respectivas áreas. Caso necessite de acesso ao diretório de outro setor, o gestor da área deverá comunicar o setor NSI mediante abertura de solicitação no sistema de chamados do NSI anexando o formulário **BH-SKM-F-001** assinado para conceder acesso ao diretório específico.

Os usuários não deverão criar sites na estrutura organizacional do SharePoint da SKEMA.

É proibida, também, a produção e armazenamento de arquivos de trabalho em nuvens não corporativas (OneDrive pessoal, Dropbox etc.) e nas próprias máquinas, por não ter garantia de backup (poderão ser perdidos caso ocorra uma falha no computador) e compartilhamento com todos os colaboradores envolvidos.

A partir da implantação desta Política, todos os arquivos que não sejam do interesse da SKEMA deverão ser retirados dos equipamentos para evitar problemas futuros com as auditorias.

5.20. BACKUP DE ARQUIVOS

Um dos procedimentos mais básicos da Segurança da Informação é a implantação de uma Política de Backup (cópia de segurança). Uma organização tem que estar preparada para recuperar (restaurar) todos os seus dados de forma íntegra caso um incidente de perda

de dados venha a ocorrer. Assim, estabelecem-se as regras:

- Todo sistema ou informação relevante para a operação dos negócios da SKEMA deve possuir cópia dos seus dados de produção para que, em eventual incidente de indisponibilidade de dados, seja possível recuperar ou minimizar os impactos nas operações da instituição;
- As áreas de negócio ficarão responsáveis por classificar os dados de acordo com a relevância e provocar o NSI sobre a necessidade de backup dos mesmos, sugerindo o tempo de retenção destas cópias;
- Todos os backups devem ser automatizados por sistemas de agendamento para que sejam, preferencialmente, executados fora do horário comercial, períodos de pouco ou nenhum acesso de usuários ou processos aos sistemas de informática;
- As mídias de backup devem ser acondicionadas em local seco, climatizado, seguro (de preferência em cofres corta-fogo segundo as normas da ABNT) e, preferencialmente, distantes o máximo possível do Datacenter;
- Toda infraestrutura de suporte aos processos de backup e restauração deve possuir controles de segurança para prevenção contra acessos não autorizados, bem como mecanismos que assegurem seu correto funcionamento;
- O NSI deve preparar semestralmente um plano para execução de testes de restauração de dados, que deve ter escopo definido em conjunto com as áreas de negócio. Por se tratar de uma simulação, o executor deve restaurar os arquivos em local diferente do original, para que assim não sobreponha os arquivos válidos;
- Na situação de erro de backup e/ou restore é necessário que ele seja feito logo no primeiro horário disponível, assim que o responsável tenha identificado e solucionado o problema. Caso seja extremamente negativo o impacto da lentidão dos sistemas derivados desse backup, eles deverão ser executados apenas mediante justificativa de necessidade.
- Todos os usuários deverão utilizar e armazenar os dados dentro da plataforma em nuvem definida pela instituição no âmbito da SKEMA GLOBAL. O NSI não se responsabiliza pela guarda, armazenamento ou restauração de arquivos que não estejam armazenados dentro do padrão da SKEMA GLOBAL.

5.21. UTILIZAÇÃO DA INTERNET

A internet foi instalada para viabilizar a busca de informações e agilizar determinados processos da SKEMA, podendo ser utilizada para fins pessoais pelos seus colaboradores, desde que não prejudique o andamento dos trabalhos.

O uso indevido do acesso à Internet é de inteira responsabilidade do usuário, que pode ser responsabilizado legalmente por eventuais danos causados. A utilização indevida da internet promove riscos significativos para os ativos de informação e, por esse motivo, torna-se imprescindível seu monitoramento e controles de uso.

A auditoria dos acessos à internet pode levar ao conhecimento dos responsáveis hierárquicos, relatórios com nomes dos usuários, páginas consultadas, tempo de consulta e o conteúdo navegado. Utilização da internet e aplicativos:

a. Viabilizar as atividades relacionadas ao trabalho, à pesquisa e à disseminação de informações de interesse da SKEMA e de suas unidades;

b. Não instalar ou acessar sites ou softwares de conteúdo impróprio ou não relacionado ao trabalho, como sites ou softwares de conversação instantânea que não seja o MS Teams (ferramenta oficial), como redes sociais (ex. Facebook, LinkedIn), sites de compras, sites de entretenimento, jogos, vídeo e música, e outras comunidades ou sites, exceto quando autorizado pela SKEMA;

c. Não baixar ou instalar programas transmissores de músicas e afins para tocadores de MP3, MP4, rádios on-line, programas P2P como Kazaa, Emule, Edonkey, dentre outros.

d. Utilizar com parcimônia os serviços de streaming;

e. Não utilizar a rede para fazer downloads ou uploads não relacionados às atividades da SKEMA ou que não sejam previamente autorizados;

f. Utilizar apenas os softwares autorizados pelo NSI para a navegação na internet.

5.22. REDES SOCIAIS, WHATSAPP E E-MAIL PESSOAIS

O uso de redes sociais, serviços de e-mail e WhatsApp e outros mensageiros pessoais nas dependências físicas da SKEMA é autorizado, desde que:

I. não sejam utilizados para acesso ou divulgação de qualquer Informações Protegidas;Não prejudique o fluxo de atividades profissionais do colaborador e de seus colegas de trabalho;
II. não sejam utilizados para acesso ou divulgação de qualquer conteúdo não autorizado por esta Política;
III. não atrapalhe o exercício das atividades do colaborador, bem como de qualquer outro colaborador;
IV. o colaborador não compartilhe, poste, divulgue ou exponha qualquer imagem, foto, vídeo ou som captado no ambiente interno da SKEMA;
V. o colaborador não compartilhe, poste, divulgue ou exponha qualquer comentário ou texto que revele ou induza terceiros a acreditar que se trata de uma opinião ou posicionamento da SKEMA; e
VI. o colaborador abstenha-se de citar, em qualquer hipótese, o nome da SKEMA ou qualquer marca relacionada ou de titularidade da SKEMA.

O colaborador é exclusivamente responsável pelo uso e guarda de suas senhas de acesso a redes sociais e e-mails pessoais, e a Companhia recomenda expressamente o

uso de navegadores anônimos para o uso de aplicações particulares em equipamentos de propriedade da SKEMA.

A SKEMA poderá suspender, temporariamente e sem aviso prévio, o uso e o acesso a essas aplicações, a seu exclusivo critério, por questões de governança e/ou de segurança da informação, independentemente de comunicação prévia ao colaborador.

5.23. JOGOS

Jogos estão terminantemente proibidos por congestionarem a rede. Eventualmente, em situações acadêmicas poder-se-á utilizar jogos desde que aprovados expressamente pelo NSI e Reitoria.

5.24. SOFTWARES

Os softwares homologados e instalados nos computadores e servidores de rede são de propriedade exclusiva da SKEMA, sendo proibidas as cópias integrais ou parciais, bem como a instalação de softwares piratas.

Pirataria é considerada crime e softwares piratas causam prejuízos tanto materiais como funcionais, além de denegrir a imagem da empresa. Por esta razão, estão terminantemente proibidos.

A instalação de softwares não autorizados (Pirataria) constitui crime contra a propriedade intelectual, de acordo com a Lei 9.609 de 19/02/98, e o infrator está sujeito à pena de detenção e multa.

A SKEMA mantém contratos especiais com alguns fabricantes de software e poderá estender a utilização de alguns deles nos computadores pessoais dos colaboradores, bastando ao colaborador solicitar a instalação ao NSI.

É proibido o uso de e-mails, correios eletrônicos ou mensagens instantâneas de forma contrária à lei, à moral, aos bons costumes, à ordem pública ou que infrinjam os direitos à propriedade intelectual ou industrial pertencente a terceiros.

O conteúdo e a utilização de e-mails, correios eletrônicos ou mensagens instantâneas deve ser de caráter exclusivamente profissional.

5.25. ACESSO FÍSICO AO CENTRO DE PROCESSAMENTO DE DADOS (CPD)

O Centro de Processamento de Dados (CPD) da SKEMA é uma área fundamental para o funcionamento da infraestrutura tecnológica da instituição.

Para resguardar a proteção e segurança do local e dos seus equipamentos, o acesso ao

CPD é restrito às pessoas devidamente autorizadas pelo NSI para a execução de atividades profissionais.

Caso seja necessário que colaboradores ou prestadores de serviços externos entrem no CPD, o NSI adotará as seguintes medidas:

- Identificar a pessoa que acessará o local;
- Registrar data e horário de entrada e saída de cada pessoa;
- Definir funcionário do NSI que estará presente durante todo o tempo de acesso para que ele atue como responsável pelo acompanhamento da atividade profissional;
- Certificar que nenhuma pessoa entre no local com quaisquer objetos que possam danificar os equipamentos;
- Permitir a entrada ou retirada de equipamentos do CPD somente com autorização prévia;
- Documentar com gravações de vídeos as dependências do CPD;
- Manter as portas do CPD sempre fechadas;
- Permitir a entrada de fornecedores e prestadores de serviço somente se autorizados pelo NSI e desde que possuam contrato vigente com a SKEMA que justifique o acesso ao CPD;
- Permitir a entrada ou retirada de equipamentos do CPD somente com autorização prévia e expressa do Gestor do NSI.

5.26. AUDITORIAS

Auditorias serão realizadas e relatórios serão gerados periodicamente.

A Diretoria da SKEMA poderá solicitar, ao NSI, relatórios de auditoria contendo o nome, mensagens trafegadas, acessos à Internet e demais informações do usuário.

Todos os usuários da rede da SKEMA estão sujeitos à auditoria de redes. Os procedimentos de auditoria e de monitoramento de uso serão realizados periodicamente ou sempre que solicitados pela diretoria ou NSI ou profissional contratado para este fim, com o objetivo de observar o cumprimento das normas deste regulamento pelos usuários da rede e com vistas à gestão de desempenho e segurança da informação.

Havendo evidência de atividade que possa comprometer a segurança da rede ou que descumpra as regras estabelecidas por este regulamento, será permitido ao administrador da rede auditar e monitorar as atividades de um usuário, além de inspecionar seus arquivos, registros de acesso, contas de e-mail corporativo e acesso aos sistemas e sites de comunicação interna da empresa, sendo o fato imediatamente comunicado à Diretoria ou seus representantes. Os dados apurados no computador serão mantidos em sigilo pela direção da SKEMA.

A SKEMA poderá, a qualquer tempo, implantar aplicativos de segurança, monitoramento

e gravação do uso da rede e internet, instalar softwares e hardwares para proteger a rede e garantir a integridade dos dados e programas, inspecionar arquivos armazenados na rede, seja em disco local, virtual ou nas áreas privadas da rede, a fim de assegurar o cumprimento das regras aqui estabelecidas.

5.27. PRESTAÇÃO DE CONTAS – RESPONSABILIZAÇÃO

A SKEMA, por via desta Política de Segurança da Informação e segundo as melhores práticas da ISO 27002:2022, no que tange ao gerenciamento dos papéis e responsabilidades pela segurança da informação, deve:

1. proteger as informações e outros ativos associados;
2. realizar os processos específicos de segurança da informação;
3. promover atividades de gestão de riscos de segurança da informação e, em especial, aceitação de riscos residuais (por exemplo, para os proprietários de risco);
4. definir todo o pessoal que utilizará as informações da organização e outros ativos associados.

Para garantir as regras mencionadas nesta PSI, a SKEMA poderá:

1. implantar sistemas de monitoramento nas estações de trabalho, servidores, correio eletrônico, conexões com a internet, dispositivos móveis ou wireless e outros componentes da rede – a informação gerada por esses sistemas poderá ser usada para identificar usuários e respectivos acessos efetuados, bem como material manipulado;
2. tornar públicas as informações obtidas pelos sistemas de monitoramento e auditoria, no caso de exigência judicial, solicitação do gerente (ou superior) ou por determinação do Comitê de Segurança da Informação;
3. realizar, a qualquer tempo, inspeção física nas máquinas de sua propriedade;
4. instalar sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações e dos perímetros de acesso.A SKEMA poderá instituir o COMITÊ DE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE para atribuir responsabilidade aos seus integrantes, bem como as ações a serem executadas dentro da organização.

5.28. DA PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS

A SKEMA realizou sua adequação às leis de privacidade e proteção de dados do Brasil e da União Europeia, tendo sua política de privacidade externa disponibilizada nas Informações Legais de seu site publicado na internet.

Quanto aos seus colaboradores, prestadores de serviços e parceiros, a SKEMA incluiu em seus instrumentos jurídicos, as normas quanto à sua política de privacidade e proteção

de dados.

Além disso, a SKEMA promove internamente a conscientização sobre privacidade e proteção dos dados, mediante treinamentos e a disponibilização da Cartilha de Proteção de Dados, com informações precípuas sobre a Lei Federal 13.709, de 14 de agosto de 2018, que dispõe sobre a lei geral de Proteção de Dados Pessoais no Brasil.

E, ainda para disseminar e manter a cultura da privacidade e proteção de dados na SKEMA, foi instituído o Comitê de Privacidade de Dados, que se reune pelo menos uma vez, a cada seis meses, podendo ainda serem realizadas reuniões extraordinárias, quando necessário, para deliberação sobre algum incidente grave ou definição relevante para a SKEMA, no que é pertinente a privacidade e proteção de dados.

Cabe também ao Comitê, propor alterações nas versões da PSI quanto à privacidade e proteção dos dados, bem como a inclusão, a eliminação ou a mudança de normas complementares, avaliar os incidentes de segurança e propor ações corretivas.

5.29. CONSCIENTIZAÇÃO EM SEGURANÇA DA INFORMAÇÃO

Um plano de conscientização da segurança da informação deve ser elaborado e executado para atingir o seguinte objetivo: *"Garantir que a Segurança da Informação não seja apenas conhecida, mas compreendida por todos os funcionários e colaboradores, conscientizando-os sobre melhores práticas, requisitos mínimos, riscos e responsabilidades existentes e quais medidas devem ser adotadas quando houver incidentes de segurança de forma a atingir uma melhor utilização e proteção à informação."*

As diretrizes básicas são:

1. Elaboração de um processo de treinamento continuado contemplando todos os níveis funcionais do Conglomerado;
2. Divulgação de diversos materiais e alertas referente a Segurança da Informação para funcionários, colaboradores e clientes;
3. Criação de procedimentos de aferição do nível de conhecimento dos usuários em geral;
4. Organização de eventos que tenham o intuito de fortalecer a conscientização sobre diversos aspectos de segurança em geral;
5. Revisão periódica do plano, adequando as ações às novas necessidades, evitando torná-lo repetitivo.

5.33. DISPOSIÇÕES FINAIS

A segurança da informação deve ser entendida como parte fundamental da cultura interna da SKEMA. Qualquer incidente de segurança subtende-se como alguém agindo

contra a ética e os valores regidos pela instituição.

Todas as práticas que sobressaltem a segurança da informação serão tratadas com a aplicação de ações disciplinares, desde uma advertência verbal até rescisão contratual por justa causa, levando em consideração fatores como: função exercida pelo colaborador, período utilizado, local de utilização, horário de utilização, prejuízo real ou potencial causado à SKEMA, além de responder legalmente por atividades que descumpram a legislação brasileira, entre outros.

5.34. CONTATOS IMPORTANTES

Para assuntos relativos aos softwares, redes e informática:

Responsável pelo NSI:Leonardo Ribeiro (leonardo.ribeiro@skema.edu)

Para assuntos relativos à restrição de acesso para pastas do servidor, bem como as regras de salvamento de arquivos, suporte a estações de trabalho, salas de aula, alunos, impressoras, eventos, portais e sistemas, o colaborador deverá solicitar ao setor NSI mediante abertura de solicitação no sistema de chamados do NSI, via e- mail: suporte@skema.edu.br ou sistemas@skema.edu.br.

Para comunicar qualquer incidência de risco ou violação de segurança da informação: dpo.brasil@skema.edu

Para comunicar qualquer demanda para o Comitê de Segurança da Informação: segurancainformacao@skema.edu

SKEMA BRASIL
POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

2024 | Belo Horizonte, Minas Gerais - Brasil