UNIVERSIDADE FEDERAL DOS VALES DO JEQUITINHONHA E MUCURI

Sistemas de Informação 5º /2020

SEGURANÇA E AUDITORIA DE SISTEMAS DE INFORMAÇÃO: TRABALHO PRÁTICO I

Grupo C:

Alex Lopes da Rocha

Guilherme Rocha

Luíz Araújo

Jose Maria Pinto

Matheus Andrade

TeamStudy Preparatórios

PSI: POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Documento de Diretrizes e Normas Administrativas

Diamantina MG - Outubro/2020

1. Dados da Empresa

Nome: TeamStudy Preparatórios.

Descrição: Uma empresa que realiza cursos preparatórios para vestibular, concursos e processos seletivos.

Data de surgimento: 05/10/2020

Tamanho: pequena (localizada em uma cidade do interior).

Número de funcionários: 7 no total, sendo 1 diretor, 1 recepcionista e 5 professores (todos os da limpeza são terceirizados).

Tipo de negócio: Escola preparatória para processos seletivos, vestibulares e concursos.

Ambiente físico: “fazer uma planta com visão de cima mesmo, contendo umas 4 salas de aula (definir quantidade de cadeiras e computadores para cada), 1 banheiro, uma sala de recepção maior (definir quantas mesas e cadeiras e outras coisas convenientes), duas salas de diretor (ou uma só onde os dois possam ficar) “

1. Planta da TeamStudy Preparatórios

2 Salas de Aula (Grandes):

- 60 cadeiras
- 4 quadros

2 salas de Aula (pequenas)

- 40 cadeiras
- 2 quadros
- 2 ventiladores

Sala de recepção

- 3 cadeiras
- 1 mesa
- 1 rack
- 1 TV
- 1 impressora
- 1 computador

Sala da Diretoria

- 3 computadores
- 4 cadeiras
- 2 armários
- 3 arquivos

- 1 impressora
- 2 racks

Sala de convivência

- 4 microondas e 2 filtros

Banheiro feminino

- 4 sanitários
- 2 pias

Banheiro Masculino

- 4 sanitários
- 2 pias

1.1 Missão

Promover e disseminar a educação para transformações de vidas e conquistas de sonhos de modo a facilitar a transmissão do conhecimento.

1.2 Visão

Tornar-se referência em ensino para concurseiros e vestibulandos no Vale do Jequitinhonha e Mucuri nos próximos 4 anos.

1.3 Valores

- Paciência
- Humildade
- Responsabilidade
- Paixão por ensinar
- Conhecimento deve ser ensinado naturalmente e não como imposição

2. Vulnerabilidades, principais ameaças, riscos e impactos

2.1)

❖ **Vulnerabilidade:**

- Recepcionista se ausentar do seu local de trabalho para ir ao banheiro, cozinha, diretoria…

❖ **Principais ameaças**:

- Alguém acessar o computador do funcionário.
- Roubo de algum pertence do funcionário ou da escola

❖ **Riscos:**

- Informações sobre estudantes, professores ou diretores vazadas.
- Dependendo do que for roubado, a escola pode sofrer danos financeiros altos

❖ **Impactos:**

- Dados de alunos podem ser vazados.
- Ter que reembolsar algum pertence

2.2)

❖ **Vulnerabilidade**:

- Documentos sobre as mesas

❖ Principais ameaças:

- Informações vazadas
- Perda de documentos

❖ Riscos:

- Processos de danos morais
- Perda no faturamento

❖ Impactos:

- confiança reduzida
- Desqualificação profissional

3)

❖ Vulnerabilidade:

- Professor se ausentar da sala de aula.

❖ Principais ameaças:

- Aluno mal intencionado obter alguma informação do computador pessoal do professor
- Tumulto na sala de aula.

❖ Riscos:

- O professor pode ter informações pessoais dele, de outrem ou da sua turma vazada, compartilhada, alterada ou apagada.
- Tumultos podem levar a brigas entre alunos.

❖ Impactos:

- Alunos podem ter que passar por revistas.
- A turma pode ser prejudicada caso alguma informação a respeito dela seja adulterada.
- Dependendo da atitude do aluno ele pode ser suspenso ou até expulso.
- Pais ou responsáveis culparem o próprio preparatório pelos danos e possivelmente abandonar a instituição.

4)

❖ Vulnerabilidade:

- Desconhecidos se passando por aluno.

❖ **Principais ameaças:**

- Segurança dos alunos em risco.
- Professores ameaçados.

❖ **Riscos:**

- Tentativa de massacre.
- Violência Sexual.
- Prejuízo financeiro.
- Roubo de informações

❖ **Impactos:**

- Indenizações para os lesados.
- Confiabilidade reduzida.

5)

❖ **Vulnerabilidade:**

- Invasão no sistema de gerenciamento do Cursinho.

❖ **Principais ameaças:**

- Acesso a dados dos alunos ou professores.
- Trocas de horários dos professores.
- mudanças de salas.

❖ **Riscos:**

- Atraso nas aulas.
- Perda de alunos.

- Mudanças de professores.

❖ **Impactos:**
- Queda no faturamento.
- Investimento em outro sistema.
- Perda dos dados da escola, estudantes e colaboradores.

3. Política de Segurança da Informação

3.1 OBJETIVOS

Estabelecer normas e diretrizes que permitam aos colaboradores da TeamStudy Preparatórios seguirem padrões de comportamento relacionados à segurança da informação adequados às necessidades de negócio e de proteção legal da empresa e do indivíduo.

Nortear a definição de normas e procedimentos específicos de segurança da informação, bem como a implementação de controles e processos para seu atendimento.

A TeamStudy Preparatórios presa pelas seguintes características:

- **Integridade:** garantia de que a informação seja mantida esteja em um formato verdadeiro e correto para seus propósitos originais, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais.
- **Confidencialidade:** garantia de que o acesso à informação seja obtido somente por pessoas autorizadas.
- **Disponibilidade:** garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário. As salas de aulas devem estar disponíveis 10 minutos antes de cada turno começar

3.2 APLICAÇÕES DA PSI

As diretrizes aqui estabelecidas deverão ser seguidas por todos os colaboradores, bem como os prestadores de serviço, e se aplicam à informação em qualquer meio ou suporte.

Esta política dá ciência a cada colaborador de que os ambientes, sistemas, computadores e redes da empresa poderão ser monitorados e gravados.

É também obrigação de cada colaborador manter-se atualizado em relação a esta PSI e aos procedimentos e normas relacionadas, buscando orientação do seu diretor sempre que não estiver absolutamente seguro quanto à aquisição, uso e/ou descarte de informações.

3.3 PRINCÍPIOS DA PSI

Toda informação produzida ou recebida pelos colaboradores como resultado da atividade profissional pertence à referida instituição. As exceções devem ser explícitas e formalizadas em contrato entre as partes.

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.

A TeamStudy Preparatórios, por meio da Gerência de Sistemas, poderá registrar todo o uso dos sistemas e serviços, visando garantir a disponibilidade e a segurança das informações utilizadas.

3.4 REQUISITOS DA PSI

Para a uniformidade da informação, a PSI deverá ser comunicada a todos os colaboradores da TeamStudy Preparatórios a fim de que a política seja cumprida dentro e fora da empresa.

- Deverá haver um comitê multidisciplinar responsável pela gestão da segurança da informação, doravante designado como Comitê de Segurança da Informação.
- Tanto a PSI quanto às normas deverão ser revistas e atualizadas periodicamente, sempre que algum fato relevante ou evento motive sua revisão antecipada, conforme análise e decisão do Comitê de Segurança.
- Todo incidente que afete a segurança da informação deverá ser comunicado inicialmente à TeamStudy Preparatórios e ela, se julgar necessário, deverá encaminhar posteriormente ao Comitê de Segurança da Informação para análise.
- Um plano de contingência e a continuidade dos principais sistemas e serviços deverão ser implantados.
- A TeamStudy Preparatórios exonera-se de toda e qualquer responsabilidade decorrente do uso indevido, negligente ou imprudente dos recursos e serviços

concedidos aos seus colaboradores, reservando-se o direito de analisar dados e evidências para obtenção de provas a serem utilizadas nos processos investigatórios, bem como adotar as medidas legais cabíveis.

- Esta PSI será implementada na TeamStudy Preparatórios é obrigatória para todos os colaboradores, independentemente do nível hierárquico ou função na empresa, bem como de vínculo empregatício ou prestação de serviço.
- 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.

3.5 DIRETRIZES

- Documentação: A documentação tem que ser sempre atualizada, todo recurso ou equipamento deve ser identificado, homologado
- Ambiente: Todo recurso como *hardware* e *software* antes de instalados devem ser plenamente testados em laboratórios específicos;
- Salas de aulas: As salas de aulas não devem ter suas estruturas físicas avariadas por quaisquer que sejam, cabendo punição no descumprimento.
- **Segurança física:** Somente funcionários poderão ter acesso a sala da direção e deverão usar crachá de identificação. Os alunos devem se identificar por meio da carteira estudantil para adentrar ao recinto, sendo proibida a permanência desses dentro da sala da direção, sem que haja motivo
- Proteção contra vírus: Qualquer arquivo recebido via redes pelos computadores institucionais, devem passar por uma verificação antivírus, este não pode ser desabilitado de forma nenhuma.

3.5.1 Dos Colaboradores em Geral

Colaborador é toda e qualquer pessoa física, contratada. Será de inteira responsabilidade de cada um, todo prejuízo ou dano que vier a sofrer ou causar à TeamStudy Preparatórios e/ou a terceiros, em decorrência da não obediência às diretrizes, normas e procedimentos aqui referidos.

3.5.2 Dos diretores de Pessoas ou dos Processos

Ser exemplar em relação à segurança da informação, servindo como modelo de conduta para os colaboradores sob a sua gestão.

Adaptar-se às normas, processos e aos procedimentos e sistemas sob sua responsabilidade atendendo a PSI, bem como aos termos da Norma Educacional e do ensino.

3.5.3 Dos detentores da Informação

3.5.3.1 - Comitê de Segurança da Informação

Deve ser formalmente constituído por colaboradores com nível hierárquico mínimo gerencial ou professor, nomeados para participar do grupo pelo período de um ano.

Cabe ao CSI:

- Propor investimentos relacionados à segurança da informação com o objetivo de reduzir mais os riscos;
- Propor alterações nas versões da PSI e a inclusão, a eliminação ou a mudança de normas complementares;
- Avaliar os incidentes de segurança e propor ações corretivas;
- Definir as medidas cabíveis nos casos de descumprimento da PSI e/ou das Normas de Segurança da Informação complementares.

4. Normas e Procedimentos

4.1 E-MAIL

O objetivo desta norma é informar aos colaboradores da TeamStudy Preparatórios quais são as atividades permitidas e proibidas quanto ao uso do e-mail corporativo e quais os procedimentos adotados.

O uso do e-mail da TeamStudy Preparatórios é para fins corporativos e relacionados às atividades do colaborador usuário dentro da empresa. A utilização desse serviço para fins pessoais é permitida desde que feita com bom senso, não prejudicando a TeamStudy Preparatórios.

Informamos que é proibido aos colaboradores o uso do e-mail da TeamStudy Preparatórios:

- Enviar mensagens não solicitadas para múltiplos destinatários, exceto se relacionadas a uso legítimo da instituição;
- Enviar mensagem por e-mail pelo endereço de seu departamento ou usando o nome de usuário de outra pessoa ou endereço de e-mail que não esteja autorizado a utilizar;
- Enviar qualquer mensagem por meios eletrônicos que torne seu remetente e/ou a TeamStudy Preparatórios ou suas unidades 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 previstas;
- Apagar mensagens pertinentes de e-mail quando qualquer uma das unidades da TeamStudy Preparatórios estiver sujeita a algum tipo de investigação.

- Produzir, transmitir ou divulgar mensagens que:
  - Contenham qualquer ato ou forneça orientação que conflite ou contrarie os interesses da TeamStudy Preparatórios;
  - Contenham ameaças eletrônicas, como: spam, mail bombing, vírus de computador;
  - Contenham 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;

- Contenha anexo(s) superior(es) a 15 MB para enviar (interno e internet) e 15MB para recebimento (internet).
- 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 e-mail sempre deverão incluir assinatura com o seguinte formato:
    - Nome do colaborador
    - Cargo
    - Telefone(s)
    - E-mail

4.2 INTERNET

As regras atuais da TeamStudy Preparatórios visam basicamente o desenvolvimento de um comportamento ético e profissional do uso da internet e os procedimentos adotados. Embora a conexão direta e permanente da rede corporativa da instituição com a internet oferece um grande potencial de benefícios, ela abre a porta para riscos significativos para
os ativos de informação.

- A rede da instituição só será acessado mediante login, isto vale tanto para internet cabeada, quanto pelo wifi. É aplicado aos colaboradores e aos estudantes
- Qualquer informação que é acessada, transmitida, recebida ou produzida na internet está sujeita a divulgação e auditoria. Portanto, a TeamStudy Preparatórios, em total conformidade legal, reserva-se o direito de monitorar e registrar todos os acessos a ela.
- A TeamStudy Preparatórios, ao monitorar a rede interna, pretende garantir a integridade dos dados e programas. Toda tentativa de alteração dos

parâmetros de segurança, por qualquer colaborador ou estudante, sem o devido credenciamento e a autorização para tal, será julgada inadequada e os riscos relacionados serão informados ao respectivo diretor. O uso de qualquer recurso para atividades ilícitas poderá acarretar as ações administrativas e as penalidades decorrentes de processos civil e criminal, sendo que nesses casos a instituição cooperará ativamente com as autoridades competentes.

- A internet disponibilizada pela instituição aos seus estudantes e colaboradores, independentemente de sua relação contratual, pode ser utilizada para fins pessoais, desde que não prejudique o andamento dos trabalhos nas unidades e não infrinja nenhuma regra da empresa ou crime tecnológico.
- É proibida a divulgação e/ou o compartilhamento indevido de informações da área administrativa e de informações dos colaboradores ou alunos, isto é imagens dos mesmos sem consentimento ou autorização da chefia imediata em listas de discussão, sites ou comunidades de relacionamento, salas de bate papo ou chat, comunicadores instantâneos ou qualquer outra tecnologia correlata que venha surgir na internet.
- O uso, a instalação, a cópia ou a distribuição não autorizada de softwares que tenham direitos autorais, marca registrada ou patente na internet são expressamente proibidos. Qualquer software não autorizado baixado será excluído, e o colaborador pode ter seu acesso a rede restringido.
- Como regra geral, materiais de cunho sexual não poderão ser expostos. Nos computadores pertencentes a escola, esse material não devem ser armazenados, distribuídos, impressos ou gravados.
- Os colaboradores e estudantes não poderão utilizar os recursos da TeamStudy Preparatórios para deliberadamente propagar qualquer tipo de vírus, worm, cavalo de troia, spam, assédio, perturbação ou programas de controle de outros computadores.
- O acesso a softwares peer-to-peer (Kazaa, BitTorrent e afins) serão permitidos, mas para fins acadêmicos, caso identificado que o usuário desrespeitou essa medida 3 vezes, tomará bloqueio do acesso a softwares peer-to-peer.

4.3 IDENTIFICAÇÃO

- Os dispositivos de identificação e senhas protegem a identidade do colaborador ou aluno, evitando e prevenindo que uma pessoa se faça passar por outra perante a TeamStudy Preparatórios e/ou terceiros.
- O uso dos dispositivos e/ou senhas de identificação de outra pessoa constitui crime tipificado no Código Penal Brasileiro (art. 307 – falsa identidade).
- O usuário, vinculado aos dispositivos na rede, será responsável pelo seu uso correto perante a instituição e a legislação (cível e criminal).
- É proibido o compartilhamento de login.
- Os usuários que não possuem perfil de administrador deverão ter senha de tamanho variável, possuindo no mínimo 6 (seis) caracteres alfanuméricos, utilizando caracteres especiais (@ # $ %) e variação entre caixa-alta e caixa-baixa (maiúsculo e minúsculo) sempre que possível(não é obrigatório).
- Já os usuários que possuem perfil de administrador ou acesso privilegiado deverão utilizar uma senha de no mínimo 8 (dez) caracteres, alfanumérica e variação de caixa-alta e caixa-baixa (maiúsculo e minúsculo) obrigatoriamente, é recomendável o uso de caracteres especiais (@ # $ %).
- É de responsabilidade de cada usuário a memorização de sua própria senha, bem como a proteção e a guarda dos dispositivos de identificação que lhe forem designados.
- As senhas não devem ser anotadas ou armazenadas em arquivos eletrônicos (Word, Excel, etc.), compreensíveis por linguagem humana (não criptografados); não devem ser baseadas em informações pessoais, como próprio nome, nome de familiares, data de nascimento, endereço, placa de veículo, nome da empresa, nome do departamento; e não devem ser constituídas de combinações óbvias de teclado, como “abcdefgh”, “87654321”, entre outras.
- Todos os acessos devem ser imediatamente bloqueados pelo diretor quando se tornarem desnecessários. Portanto, assim que algum colaborador for demitido ou solicitar demissão, ou estudante for desmatriculado ou concluinte.

4.4. COMPUTADORES E RECURSOS TECNOLÓGICOS

- Os equipamentos disponíveis aos colaboradores de propriedade da TeamStudy Preparatórios devem ser utilizados e manuseados corretamente para as atividades de interesse da instituição.
- A TeamStudy Preparatórios, na qualidade de proprietário dos equipamentos fornecidos, reserva-se o direito de inspecioná-los a qualquer tempo, caso seja necessário realizar uma manutenção de segurança.
- Os computadores devem ter versões do software antivírus instaladas, ativas e atualizadas permanentemente. O usuário, em caso de suspeita de vírus ou problemas na funcionalidade, deverá acionar o diretor, para este tomar as decisões cabíveis.
- Documentos imprescindíveis para as atividades dos colaboradores da instituição deverão ser salvos em drives de rede. Tais arquivos, se gravados apenas localmente nos computadores (por exemplo, no drive C:), não terão garantia de backup e poderão ser perdidos caso ocorra uma falha no computador, sendo, portanto, de responsabilidade do próprio usuário.
- Os colaboradores da TeamStudy Preparatórios e/ou detentores de contas privilegiadas não devem executar nenhum tipo de comando ou programa que venha sobrecarregar os serviços existentes na rede corporativa sem a prévia solicitação e a autorização da Gerência de Sistemas.
- Todos os computadores de uso individual deverão ter senha para restringir o acesso de colaboradores não autorizados. Os colaboradores devem informar ao departamento técnico qualquer identificação de dispositivo estranho conectado ao seu computador.
- Todos os modems internos ou externos devem ser removidos ou desativados para impedir a invasão/evasão de informações, programas, vírus. Em alguns casos especiais, conforme regra específica, será considerada a possibilidade de uso para planos de contingência mediante a autorização dos diretores das áreas e da área de informática.
- O transporte dos equipamentos deve ser feito com autorização do CSI. O empréstimo de equipamentos para os colaboradores deve ter permissão mínima do Diretor da TeamStudy, tendo como responsabilidade por eventuais estragos, perdas ou roubos ambas as partes.

4.5 Dispositivos móveis

A TeamStudy Preparatórios deseja facilitar a mobilidade e o fluxo de informação entre seus colaboradores. Por isso, permite que eles usem equipamentos portáteis. 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.

- 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, ou qualquer imagem de aluno não autorizada pelos pais, maiores de idade ou responsáveis, mesmo depois de terminado o vínculo contratual mantido com a instituição.
- É permitido o uso de rede banda larga na rede da instituição por motivos de pesquisa e comunicação com colaboradores da instituição.
- O colaborador ou estudante deverá estar ciente de que o uso indevido do dispositivo móvel dentro da instituição caracteriza 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 TeamStudy Preparatórios e/ou a terceiros.
- Equipamentos portáteis, como smartphones, palmtops, pen drives e players de qualquer espécie, quando não informados e autorizados pelo comitê de segurança ou pela chefia superior, não serão validados para uso e conexão em sua rede corporativa.

4.6 BACKUP

- Todos os backups devem ser automatizados por sistemas de agendamento automatizado para que sejam preferencialmente executados fora do horário comercial, nas chamadas “janelas de backup” – períodos em que não há nenhum ou pouco acesso de usuários ou processos automatizados aos sistemas de informática.

- As mídias de backup (como DAT, DLT, LTO, DVD, CD e outros) devem ser acondicionadas em local seco, climatizado, seguro (de preferência em cofres corta-fogo segundo as normas da ABNT) e distantes o máximo possível do Datacenter.
- As fitas de backup devem ser devidamente identificadas, inclusive quando for necessário efetuar alterações de nome, e de preferência com etiquetas não manuscritas, dando uma conotação mais organizada e profissional.
- O tempo de vida e uso das mídias de backup deve ser monitorado e controlado pelos responsáveis, com o objetivo de excluir mídias que possam apresentar riscos de gravação ou de restauração decorrentes do uso prolongado, além do prazo recomendado pelo fabricante.
- As mídias de backups históricos ou especiais deverão ser armazenadas em instalações seguras.
- 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.
- 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.

4.7 RESPONSABILIDADE

Assim como tendo conhecimento das informações normas e procedimentos relatados, tem se a ética e a segurança a serem entendidas como parte fundamental da cultura interna da TeamStudy Preparatórios. Ou seja, qualquer incidente de segurança subtende-se como alguém agindo contra a ética e os bons costumes regidos pela instituição será punido de acordo com as legislação vigente do Brasil.