1 INTRODUÇÃO

A Fundação Carlos Alberto Vanzolini (FCAV) reconhece a importância da Segurança da Informação como ferramenta para cumprimento da sua missão, aspiração e valores, bem como investe constantemente no crescimento profissional de seus colaboradores e em tecnologias que garantam a excelência de seus produtos e serviços.

A Política de Segurança da Informação (PSI) é o documento que orienta e estabelece as diretrizes corporativas da FCAV para a proteção dos ativos de informação e a prevenção de responsabilidade legal para todos os usuários. Deve, portanto, ser cumprida e aplicada em todas as áreas da instituição.

Por isso, é essencial a proteção dos seus ativos, uma vez que quando utilizados de modo indevido podem gerar danos irreparáveis à FCAV, além de afetar a sua imagem perante o mercado. Deste modo, preservar ativos como: a informação, equipamentos tecnológicos e a sua reputação se tornam essencial.

A PSI está baseada nas recomendações propostas pela norma ISO/IEC 27001:2013, ISO/IEC 27002:2013 e ISO/IEC 27701:2020, reconhecida mundialmente como um código de prática para a gestão da segurança da informação, bem como está de acordo com as leis vigentes em nosso país.

2 ESCOPO

Esta Política de Segurança da Informação (PSI) tem como objetivos:

Declarar formalmente o comprometimento da Direção da FCAV na promoção de diretrizes estratégicas, responsabilidades, competências, a fim de garantir a proteção dos seus ativos tangíveis e intangíveis.

Estabelecer as diretrizes que permitam aos colaboradores e clientes da FCAV 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.

Preservar as informações da FCAV quanto à:

- ✔ **Integridade:** garantia de que a informação seja mantida em seu estado original, 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.

3 ABRANGÊNCIA

Este é um documento interno, com valor jurídico e aplicabilidade imediata e indistinta, a partir de sua publicação, aos colaboradores, parceiros e fornecedores da FCAV.

4 REFERÊNCIAS

- ISO/IEC 27001:2013;
- ISO/IEC 27002:2013;
- ISO/IEC 27701:2020.

5 DEFINIÇÕES

- **Ameaça:** Causa potencial de um incidente indesejado, que pode resultar em dano.
- **Aplicativos de Comunicação:** Conjunto de código e instruções compiladas, executados ou interpretados por um Recurso de Tecnologia da Informação e Comunicação, armazenados em um dispositivo ou na nuvem, que são usados para troca rápida de mensagens, conteúdos e informações multimídia.
- **Ativo:** É qualquer coisa que tenha valor e precisa ser adequadamente protegido.
- **Ativo Intangível:** Todo elemento que possui valor e que esteja em suporte digital ou se constitua de forma abstrata, mas registrável ou perceptível, a exemplo, mas não se limitando à dados, reputação, imagem, marca e conhecimento.
- **Autenticidade:** Garantia de que a informação é procedente e fidedigna, sendo capaz de gerar evidências não repudiáveis da identificação de quem a criou, editou ou emitiu.
- **Backup:** Salvaguarda de informações realizada por meio de reprodução e/ou espelhamento de uma base de arquivos com a finalidade de recuperação em caso de incidente ou necessidade de restauração, ou ainda, constituição de infraestrutura de acionamento imediato em caso de incidente ou necessidade justificada.
- **Colaborador:** Toda e qualquer pessoa física, contratada CLT ou prestadora de serviço por intermédio de pessoa jurídica ou não, que exerça alguma atividade dentro ou fora da instituição.
- **Confidencialidade:** Garantia de que as informações sejam acessadas somente por aqueles expressamente autorizados e que sejam devidamente protegidas do conhecimento alheio.
- **Disponibilidade:** Garantia de que as informações e os Recursos de Tecnologia da Informação e Comunicação estejam disponíveis sempre que necessário e mediante a devida autorização para seu acesso ou uso.

- **Dispositivos Móveis:** equipamentos que podem ser facilmente transportados devido a sua portabilidade, com capacidade de registro, armazenamento ou processamento de informações, além da possibilidade de estabelecer conexões com a Internet e outros sistemas, redes ou qualquer dispositivo.

- **Dispositivos Removíveis de Armazenamento de Informação:** Dispositivos capazes de armazenar informações que pode ser removida do equipamento, possibilitando a portabilidade dos dados, como CD, DVD e pen drive.

- **Gestor da informação:** Colaborador responsável pela criação/recebimento, classificação, divulgação, compartilhamento, eliminação e destruição da informação. Também é incumbido da gestão de validação, liberação e cancelamento dos acessos à informação destes. Vale ressaltar que tais atividades podem ser delegadas para outro colaborador, desde que concedidas pelo Gestor da informação.

- **Homologação:** Processo de avaliação e aprovação técnica de Recursos de Tecnologia da Informação e Comunicação para serem utilizados dentro do ambiente da organização.

- **Identidade Digital:** É a identificação do colaborador em ambientes lógicos, sendo composta por seu nome de usuário (login) e senha ou por outros mecanismos de identificação e autenticação como crachá magnético, certificado digital, token e biometria.

- **Incidente de Segurança da Informação e Comunicação**: Ocorrência identificada de um estado de sistema, dados, informações, serviço ou rede, que indica possível violação à Política de Segurança da Informação ou Normas Complementares, falha de controles ou situação previamente desconhecida, que possa ser relevante à segurança da informação.

- **Informação:** Conjunto de dados que, processados ou não, podem ser utilizados para produção, transmissão e compartilhamento de conhecimento, contidos em qualquer meio, suporte ou formato.

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

- **Internet:** Rede mundial de computadores interconectada pelo protocolo TCP/IP cuja infraestrutura tem caráter aberto e colaborativo, acessível por meio de dispositivos com conexão e autorizações suficientes e que permite obter informação de qualquer outro dispositivo que também esteja conectado à rede, desde que configurado adequadamente.

- **Legalidade:** Garantia de que todas as informações sejam criadas e gerenciadas de acordo com as disposições do Ordenamento Jurídico em vigor.

- **Podcast:** são arquivos de áudio que podem ser baixados e consumidos a qualquer momento.

- **Proxy:** é um servidor que recebe as requisições de um usuário e as passa para frente, dessa forma alterando o remetente da mensagem com o objetivo de filtrar o conteúdo ou enviar

dados anonimamente. Para facilitar o entendimento, imagine que um usuário (U) se conecte a um servidor proxy (P) e faz uma pesquisa no Google, que usa um algoritmo de buscas utilizando o perfil do usuário como base.

- ✔ **Recursos de Tecnologia da Informação e Comunicação (Recursos de TIC**): hardware, software, serviços de conexão e comunicação ou de infraestrutura física necessários para criação, registro, armazenamento, manuseio, transporte, compartilhamento e descarte de informações.

- ✔ **Repositórios Digitais (Cyberlockers**): Plataformas de armazenamento na Internet, a exemplo de Google Drive, OneDrive, Dropbox, iCloud, Box, SugarSync, Slideshare e Scribd.

- ✔ **Risco:** Combinação da probabilidade da concretização de uma ameaça e seus potenciais impactos.

- ✔ **Segurança da Informação:** é a preservação da confidencialidade, integridade, disponibilidade, legalidade e autenticidade da informação. Visa proteger a informação dos diversos tipos de ameaças para garantir a continuidade dos negócios, minimizar os danos aos negócios, maximizar o retorno dos investimentos e de novas oportunidades de transação.

- ✔ **Senha de Bios:** O Sistema Básico de Entrada e Saída, o famoso **BIOS**, é um aplicativo responsável pela execução de várias tarefas no seu computador. Ele contém todo o software básico, necessário para inicializar a placa-mãe, verificar os dispositivos instalados e carregar o sistema operacional.

- ✔ **Service Desk:** é a evolução do help desk, pois possui abrangência e qualidade maiores para atender a demanda. Service Desk serve para centralizar as necessidades de uma empresa em um único lugar, registrando entrada e saída de pedidos de suporte e manutenção, para ter um maior controle sobre o que foi feito.

- ✔ **Softwares peer-to-peer:** (do inglês par-a-par ou simplesmente ponto-a-ponto, com sigla P2P) é uma arquitetura de redes de computadores onde cada um dos pontos ou nós da rede funciona tanto como cliente quanto como servidor, permitindo compartilhamentos de serviços e dados sem a necessidade de um servidor central. Uma rede peer-to-peer é mais conveniente para o armazenamento de objetos imutáveis, seu uso em objetos mutáveis é mais desafiador, e pode ser resolvido com a utilização de servidores confiáveis para gerenciar uma sequência de versões e identificar a versão corrente, pode ser usada para compartilhar músicas, vídeos, imagens, dados, enfim qualquer coisa com formato digital. Um exemplo de transmissão de dados via peer-to-peer são os Torrents.

- ✔ **Spam:** é o termo usado para referir-se aos e-mails não solicitados, que geralmente são enviados para um grande número de pessoa.

- ✔ **Tentativa de Burla:** A tentativa de burlar as diretrizes e controles estabelecidos, quando constatada, deve ser tratada como uma violação.

- **Trilhas de auditoria:** uma técnica que permite o acompanhamento de todas as atividades que afetam um determinado conjunto de informações, como um registro de dados, desde o momento em que ele entra no sistema até o instante em que é removido. As trilhas de auditoria permitem documentar, por exemplo, quem efetuou uma determinada alteração e quando isso ocorreu.

- **Violação:** Qualquer atividade que desrespeite as regras estabelecidas nos documentos normativos.

- **Worm:** é um programa capaz de se propagar automaticamente através de redes, enviando cópias de si mesmo de computador para computador

6 A POLÍTICA

a) Aplicações

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

Esta PSI dá ciência a cada colaborador de que os ambientes, sistemas, computadores e redes da empresa poderão ser monitorados e gravados, com prévia informação, conforme previsto nas leis brasileiras. Também é obrigação de cada colaborador manter-se atualizado em relação a esta PSI e aos procedimentos operacionais relacionados, buscando orientação do seu gestor ou da Área de Tecnologia da Informação (T.I.) sempre que não estiver absolutamente seguro quanto à aquisição, uso e/ou descarte de informações.

b) Princípios

Preservar e proteger a informação da FCAV ou sob sua responsabilidade, em todo o seu ciclo de vida, contida em qualquer suporte ou formato, de vulnerabilidades e ameaças;

Prevenir e reduzir impactos gerados pelos incidentes de segurança da informação, assegurando a confidencialidade, integridade, disponibilidade, autenticidade e legalidade no desenvolvimento das atividades profissionais;

Zelar por relações transparentes e éticas e coibir toda forma de corrupção, fraude, suborno, favorecimento e extorsão praticados por colaboradores;

Cumprir a legislação brasileira e os demais instrumentos regulamentares relacionados ao negócio no que diz respeito à segurança da informação.

Toda informação produzida ou recebida pelos colaboradores como resultado da atividade profissional contratada pela FCAV pertence à instituição. As exceções, quando existentes, são explícitas e formalizadas em contrato entre as partes.

7 REQUISITOS

Interpretação: Esta PSI e seus documentos complementares devem ser interpretados de forma restritiva, ou seja, as atividades que não estão tratadas nos normativos só devem ser realizadas após prévia e formal autorização do Gestor do colaborador.

Publicidade: Esta PSI e seus documentos complementares devem ser divulgados aos colaboradores pela Área de Recursos Humanos e da Área de Comunicação em conjunto com a Área de Tecnologia da Informação, visando dar publicidade para todos que se relacionam profissionalmente com a FCAV.

Propriedade: As informações geradas, acessadas, manuseadas, armazenadas ou descartadas no exercício das atividades realizadas pelos colaboradores, bem como os demais ativos intangíveis e tangíveis disponibilizados, são de propriedade ou estão sob a responsabilidade e direito de uso exclusivo a FCAV e devem ser utilizados unicamente para fins profissionais.

Propriedade Intelectual: A utilização de obras intelectuais, softwares, desenhos industriais, marcas, identidade visual ou qualquer outro sinal distintivo atual ou futuro a FCAV em qualquer suporte, inclusive na Internet e mídias sociais, deve ser previamente autorizada pela empresa e vinculada as atividades profissionais.

Classificação da Informação: Todas as informações de propriedade ou sob a responsabilidade a FCAV devem ser classificadas e protegidas com controles específicos em todo o seu ciclo de vida.

Sigilo: É vedada, a qualquer tempo, a revelação de informação de propriedade ou sob a responsabilidade a FCAV sem a prévia e formal autorização do Gestor da Informação, excetuando-se a informação pública.

Uso dos Ativos: Os ativos de propriedade ou sob sua responsabilidade a FCAV devem ser utilizados somente para fins profissionais e de acordo com as orientações dos fabricantes e da empresa.

- ✔ **Uso dos Recursos de TIC:** Os Recursos de TIC de propriedade ou sob a responsabilidade a FCAV devem ser utilizados somente para fins profissionais, de modo lícito, ético e moral e conforme as regras a FCAV.
- ✔ **Manutenção dos Ativos:** A gestão dos ativos na FCAV deve atender às recomendações dos fabricantes e desenvolvedores, sendo que qualquer necessidade de manutenção, atualização ou correção de falhas técnicas somente pode ser realizada pelo Departamento de TI, de acordo com o tipo de ativo.
- ✔ **Inventário dos Ativos:** A FCAV deve realizar inventário de hardwares e softwares que possuir, devendo o Departamento de TI indicar as informações necessárias e ser a responsável pelo seu registro, armazenamento e atualização.
- ✔ **Dispositivos Móveis Corporativos:** Os dispositivos móveis devem ser utilizados quando fornecidos ou autorizados prévia e expressamente pelo Diretor da Área/Gerência do colaborador e aprovado pela Diretoria, conforme a função do colaborador e as necessidades do negócio.

Uso dos Recursos de TIC/Dispositivos Móveis Particulares: Não é permitido o uso de Recursos de TIC/Dispositivos Móveis particulares na execução de qualquer atividade profissional, exceto quando autorizado e fundamentado pelo [NOME DO CARGO] e aprovado pelo [NOME DO CARGO/ÁREA].

Repositórios Digitais e Dispositivos Removíveis: É vedado aos colaboradores o uso de repositórios digitais ou dispositivos removíveis não autorizados ou homologados pela FCAV para armazenar ou transmitir informações de propriedade ou sob a responsabilidade da empresa.

Aplicativos de Comunicação Instantânea: O uso de aplicativos de comunicação instantânea para troca de informações corporativas deve atender as regras estabelecidas pela Área de Tecnologia da Informação.

Mídias Sociais: O uso das mídias sociais para realização das atividades profissionais em favor a FCAV deve ocorrer somente quando necessário e de forma restrita aos objetivos do negócio, de acordo com o Código de Conduta e Ética vigente. Tais atividades devem ser executadas por meio dos Recursos de TIC da FCAV.

- ✔ **Conduta do Colaborador no Uso das Mídias Sociais:** O colaborador deve ser cauteloso, ético e seguro em relação à sua exposição de modo que não afete a reputação a FCAV, a exemplo de rotinas, trajetos e contatos, além do dever de preservar o sigilo profissional nas mídias sociais.

Controle de Acesso: A FCAV controla o acesso físico e lógico aos seus ambientes, ativos e informações. Desse modo, o colaborador recebeu uma identidade digital de uso individual, intransferível e, sempre que aplicável, de conhecimento exclusivo.

- ✔ O colaborador é responsável pelo uso, proteção e sigilo de sua identidade digital, não sendo permitido compartilhar, revelar, salvar, replicar, publicar ou fazer uso não autorizado de suas credenciais, tal qual de terceiros.
- ✔ Para garantir o controle de acesso aos ambientes físicos e lógicos a FCAV, utiliza os critérios do mínimo conjunto necessário (least privilege) e estritamente necessários (need to know) ao definir os acessos de cada colaborador.

Ambientes Lógicos: Os sistemas e Recursos de TIC que suportam os processos e as informações a FCAV devem ser confiáveis, íntegros, seguros e disponíveis a quem deles necessitem para execução de suas atividades profissionais. Para garantir a segurança acima estabelecida, a FCAV utiliza os seguintes sistemas de proteção, ativos e atualizados:

- ✔ Contra programas maliciosos e acessos indevidos, como antivírus,firewall, waf, lockdown, entre outros;
- ✔ Para indicar tentativas de intrusão realizada aos ambientes lógicos, como Sistemas de Detecção a Intrusão (Intrusion Detection Systems) ou IPS (Intrusion Protection Systems);
- ✔ Contra mensagens eletrônicas indesejadas ou não autorizadas, como AntiSpam.

Ambientes Físicos: A FCAV deve estabelecer perímetros de segurança para proteção de seus ativos, especialmente aqueles que processam ou armazenam informações/ativos críticos para o negócio, e implementar controles para identificação e registro de acessos aos seus ambientes.

Áudio, Vídeos e Imagens: É vedado aos colaboradores qualquer atividade relacionada a captura de áudio, vídeo ou imagens dentro das dependências a FCAV, sem a prévia e formal autorização da Área de Comunicação e Marketing, exceto em eventos oficiais da empresa.

Contratação de Colaboradores e Prestadores de Bens e Serviços: As contratações em que ocorram o compartilhamento de informações de propriedade ou sob a responsabilidade a FCAV ou a concessão de acesso aos seus ambientes ou ativos críticos, devem ser precedidos por termos de confidencialidade e cláusulas contratuais relacionadas à segurança da informação.

Desenvolvimento e Aquisição de Software: Tanto o desenvolvimento interno e externo de softwares como aquisições de mercado devem garantir o cumprimento dos requisitos de segurança da informação e controles de acesso previstos nesta PSI e demais Normas Complementares, além de serem realizadas somente pelo Departamento de TI.

Salvaguarda (backup): A FCAV mantém um processo de salvaguarda das informações e dos dados necessários para completa recuperação dos seus sistemas (backup), a fim de atender os requisitos operacionais e legais, além de garantir a continuidade do negócio em caso de falhas ou incidentes ou sua recuperação o mais rápido possível.

Análise dos Processos e Recursos de TIC: A Área de Tecnologia da Informação deve analisar seus processos e Recursos de TIC, em intervalos regulares, visando assegurar que estejam devidamente inventariados e com seus gestores identificados e cientes, assim como suas vulnerabilidades e ameaças de segurança mapeadas.

Monitoramento: A FCAV monitora seus ambientes físicos e lógicos, visando a eficácia dos controles implantados, a proteção de seu patrimônio, a reputação e a identificação de eventos ou alertas de incidentes referentes à segurança da informação.

Auditoria e Inspeção: A FCAV pode auditar ou inspecionar os Recursos de TIC que estiverem em suas dependências ou que interajam com seus ambientes lógicos sempre que considerar necessário, atendendo aos princípios da proporcionalidade, razoabilidade e privacidade de seus proprietários ou portadores.

Gestão de Risco: O Departamento de TI deve identificar e avaliar os riscos relacionados à segurança da informação e adotar as melhores práticas para o seu gerenciamento.

Gestão de Mudança: O andamento e o resultado de uma mudança, principalmente nos sistemas e na infraestrutura tecnológica da FCAV, devem preservar os controles relacionados a disponibilidade, integridade, sigilo e autenticidade das informações e realizados somente pelo Departamento de TI.

Continuidade do Negócio: Os procedimentos de gestão de Continuidade do Negócio devem ser executados em conformidade com os requisitos de segurança da informação a FCAV.

Investimentos: Os investimentos em segurança da informação na FCAV devem ser estudados e deliberados pelo Departamento de TI junto à Diretoria, alinhado com as áreas de negócio,

considerando a viabilidade dos investimentos (custo x benefício) e os impactos de sua aplicação à qualidade dos processos de negócio.

Comitê de Segurança da Informação (CSI): A FCAV deve estabelecer um CSI responsável por assessorar e gerenciar a implementação dos controles estabelecidos pelo SGSI, analisar questões específicas ao tema, auxiliar com a melhoria constante dos padrões e observância dos normativos de segurança da informação, além de tratar questões relacionadas ao uso indevido dos ativos da empresa, interno ou externo.

- ✔ O CSI deve ser composto por uma equipe multidisciplinar, submetido à Diretoria da FCAV, com atuação permanente, reunindo-se periodicamente, conforme a necessidade, para tratar de pautas relacionadas à segurança da informação.
  - ✔ É formalmente constituído por colaboradores com nível hierárquico mínimo gerencial, nomeados para participar do grupo pelo período de um ano. A composição mínima deve incluir um colaborador de cada uma das áreas da instituição.
  - ✔ O CSI reúne-se formalmente, pelo menos uma vez a cada seis meses. Reuniões extraordinárias são realizadas sempre que houver alguma mudança no contexto externo ou interno da organização e ainda, quando for necessário deliberar sobre: algum incidente grave que comprometeu a segurança da informação, definição relevante ou necessidade de revisão desta PSI.
  - ✔ O CSI poderá utilizar especialistas, internos ou externos, para apoiarem nos assuntos que exijam conhecimento técnico específico.

Comunicação de Incidentes: A FCAV possui um canal de comunicação divulgado aos seus colaboradores para reportar possíveis casos de incidentes de segurança da informação: suportelgpd@vanzolini.org.br .

Proteção de Dados Pessoais: A FCAV respeita a privacidade. Assim deve garantir a disponibilidade, integridade e confidencialidade dos dados pessoais, em todo o seu ciclo de vida, em qualquer formato de armazenamento ou suporte, tendo o mesmo nível de tratamento de informações confidenciais. A FCAV deve avaliar as seguintes medidas de segurança da informação quanto à tratamento de dados pessoais:

- ✔ Tratamento autorizado nos termos da legislação de proteção de dados pessoais vigente;
- ✔ Adoção de medidas de segurança para proteger os dados pessoais de acesso não autorizados, situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou tratamento inadequado ou ilícito;
- ✔ Elaboração de plano de análise e resposta às violações de dados pessoais;
- ✔ Armazenamento de modo seguro, controlado e protegido, especialmente quando se tratar de dados pessoais sensíveis;
- ✔ Processos de anonimização e pseudonimização, sempre que necessário;
- ✔ Protocolos de criptografia na transmissão e armazenamento, quando verificado necessário;
- ✔ Registro lógico das operações de tratamento de dados pessoais;
- ✔ Descarte seguro dos dados pessoais ao término de sua finalidade e sua conservação de acordo com as hipóteses legais e regulatórias;
- ✔ Transferência aos Agentes de Tratamento de modo seguro e contratualmente previsto;
- ✔ Mapeamento e manutenção de inventário de fluxos de dados pessoais;
- ✔ Elaboração de relatórios de impacto à proteção de dados pessoais, quando necessário;

- ✔ Gestão e tratamento adequado de incidentes que envolvam dados pessoais;

Capacitação: A FCAV deve estabelecer um plano periódico e anual de capacitação direcionado ao desenvolvimento e manutenção das habilidades dos colaboradores sobre segurança da informação.

Revisão e Atualização: A FCAV deve possuir e manter um programa de revisão/atualização desta PSI e das Normas Complementares sempre que se fizer necessário, desde que não exceda o período máximo de 12 (dozes) meses, visando à garantia que todos os requisitos de segurança técnicos e legais implementados estejam sendo cumpridos e atualizados.

Alterações: As alterações desta PSI e das Normas Complementares devem ser devidamente comunicadas aos colaboradores.

Exceções: As exceções somente são admitidas de forma excepcional a essa PSI, devendo ser temporárias e aprovadas previamente pelo Diretor para produzirem efeito.

- ✔ Os pedidos de exceção devem ser encaminhados por escrito ao Gestor do colaborador e, se julgado pertinente, será remetido ao Diretor para análise de viabilidade. Se necessário, o pedido de exceção será submetido à Diretoria Executiva para aprovação ou denegação.
- ✔ As exceções podem ser revogadas a qualquer tempo por mera liberalidade do Gestor do colaborador ou do Diretor, devendo as Áreas relacionadas serem informadas imediatamente da denegação por quem a fez para providências, sob pena de responsabilização de quem se omitiu de eventuais prejuízos sofridos pela FCAV, seus clientes ou terceiros.

Dúvidas: Qualquer dúvida relativa a esta PSI deve ser encaminhada a Área de Tecnologia da Informação por meio do endereço eletrônico: suportelgpd@vanzolini.org.br

8 DAS RESPONSABILIDADES ESPECÍFICAS

8.1.1 Dos Colaboradores em Geral e em Regime de Exceção (Temporários)

Entender os riscos associados à sua condição especial e cumprir rigorosamente o que está previsto na PSI.

Estar ciente e manter-se atualizado com esta PSI e demais documentos complementares;

Conhecer e assinar o “Termo de Ciência e Responsabilidade”;

Utilizar os ativos de propriedade a FCAV ou sob sua responsabilidade de acordo com as orientações do fabricante, do desenvolvedor e da empresa, com cuidado e zelo;

Utilizar os ativos e informações a FCAV somente para fins profissionais, de forma ética e legal, respeitando os direitos e as permissões de uso concedidas;

Preservar a integridade, a disponibilidade, a confidencialidade, autenticidade e a legalidade das informações acessadas ou manipuladas, não as utilizando, enviando, transmitindo ou compartilhando indevidamente, em qualquer local ou mídia, inclusive na Internet;

Não revelar qualquer informação de propriedade ou sob a responsabilidade a FCAV sem a prévia e formal autorização;

Utilizar as marcas e outros sinais distintivos, patentes, desenhos industriais, softwares e demais direitos de propriedade intelectual de titularidade a FCAV somente para finalidades profissionais e autorizadas pela empresa, de acordo com a atividade e função exercida;

Zelar pela segurança da sua identidade digital, não compartilhando, divulgando ou transferindo a terceiros;

Responder por toda e qualquer atividade realizada nos Recursos de TIC a FCAV realizada mediante o uso de sua identidade digital;

Cumprir a legislação nacional vigente e demais instrumentos regulamentares relacionados às atividades profissionais;

Reportar formalmente ao seu Gestor quaisquer eventos relativos à violação ou possibilidade de violação de segurança ou atividades suspeitas.

8.1.2 Gestores

Garantir e gerenciar o cumprimento desta PSI e demais documentos complementares pelos seus colaboradores;
Ter postura exemplar em relação à segurança da informação, servindo como modelo de conduta para os colaboradores sob a sua gestão.

Atribuir aos colaboradores, na fase de contratação e de formalização dos contratos individuais de trabalho, de prestação de serviços ou de parceria, a responsabilidade do cumprimento da PSI da FCAV.

Exigir dos colaboradores a assinatura da Declaração de Compromisso e Ciência, assumindo o dever de seguir as normas estabelecidas, bem como se comprometendo a manter sigilo e confidencialidade, mesmo quando desligado, sobre todos os ativos de informações da FCAV.

Antes de conceder acesso às informações da instituição, exigir a assinatura do Acordo de Confidencialidade dos colaboradores casuais e prestadores de serviços que não estejam cobertos por um contrato existente, por exemplo, durante a fase de levantamento para apresentação de propostas comerciais.

Adaptar as normas, os processos, procedimentos e sistemas sob sua responsabilidade para atender a esta PSI.

Identificar e medir as vulnerabilidades e ameaças nos processos e atividades de sua responsabilidade, as quais devem ser tratadas diligentemente de modo a reduzir os impactos ao negócio;

Autorizar, ou não, a utilização de Recursos de TIC ou dispositivos móveis particulares por seus colaboradores para execução de qualquer atividade profissional na FCAV;

Garantir que os ativos de propriedade ou sob a responsabilidade a FCAV sejam utilizados com cuidado e de acordo com as orientações do fabricante e da empresa;

Aplicar, após definição com o Departamento de Recursos Humanos, as sanções de violação desta PSI e documentos complementares;

Identificar incidentes de segurança da informação ou qualquer ação duvidosa praticada por seus colaboradores, comunicando a área de TI imediatamente.

8.1.3 Consultoria Jurídica

Participar, apoiar e orientar, de acordo com os aspectos jurídicos, os processos de contratação e as exigências legislativas relacionadas à segurança da informação;

Validar as minutas que devem atender aos controles de segurança da informação aplicáveis aos contratos.

8.1.4 Recursos Humanos

Realizar campanhas de capacitação e divulgação da segurança da informação;

Estipular controles de segurança especificamente relacionados aos processos de contratação, encerramento e modificação das atividades dos colaboradores;

Garantir a publicidade e disponibilidade dos documentos;

Disponibilizar os normativos da FCAV, além de custodiar e colher assinatura do “Termo de Ciência e Responsabilidade” na admissão de novos colaboradores.

8.1.5 Comunicação e Marketing

Autorizar ou não, o uso das marcas, identidade visual e qualquer outro sinal distintivo atual ou futuro a FCAV;

Autorizar ou não, a gravação de áudio, vídeo ou foto das dependências a FCAV.

8.1.6 Da Área de Tecnologia da Informação

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 FCAV.

Publicar e promover as versões da PSI aprovadas pelo Comitê de Segurança da Informação.

Promover a conscientização dos colaboradores em relação à relevância da segurança da informação para o negócio da FCAV, 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.

Analisar criticamente incidentes em conjunto com o Comitê de Segurança da Informação.

Apresentar as atas e os resumos das reuniões do Comitê de Segurança da Informação, destacando os assuntos que exijam intervenção do próprio comitê ou de outros membros da diretoria.

Manter comunicação efetiva com o Comitê de Segurança da Informação sobre assuntos relacionados ao tema que afetem ou tenham potencial para afetar a FCAV.

Buscar alinhamento com as diretrizes corporativas da instituição.

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 requisitos de segurança estabelecidos por esta PSI.

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, incluindo o ambiente educacional, 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 FCAV.

Implantar controles que gerem registros auditáveis para retirada e transporte de mídias das informações custodiadas pela TI, 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 TI, garantir que as informações do usuário que tinha o ativo movimentado 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:

- ✔ os usuários (logins) individuais de funcionários serão de responsabilidade do próprio funcionário.
- ✔ os usuários (logins) de terceiros serão de responsabilidade do gestor da área contratante.

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 empresa 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 corporativo, bem como em ambiente exclusivamente educacional, exigindo o seu cumprimento dentro da empresa.

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 empresa, incidente, investigação ou outra situação que exija medida restritiva para fins de salvaguardar os ativos da empresa.
Garantir que todos os servidores, estações e demais dispositivos com acesso à rede da empresa operem com o relógio sincronizado com os servidores de tempo oficiais do governo brasileiro.

Monitorar o ambiente de TI, gerando indicadores e históricos de:

- ✔ uso da capacidade instalada da rede e dos equipamentos;
- ✔ tempo de resposta no acesso à internet e aos sistemas críticos da FCAV;
- ✔ períodos de indisponibilidade no acesso à internet e aos sistemas críticos da FCAV;
- ✔ incidentes de segurança (vírus, trojans, furtos, acessos indevidos, e assim por diante);
- ✔ atividade de todos os colaboradores durante os acessos às redes externas, inclusive internet (por exemplo: sites visitados, e-mails recebidos/enviados, upload/download de arquivos, entre outros);

8.1.7 Do Comitê de Segurança da Informação (CSI)

Instaurar, quando couber, procedimento disciplinar para apuração de responsabilidades dos envolvidos em violações de segurança da informação, e aplicar as penalidades, quando necessário.

8.1.8 Encarregado pelo Tratamento de Dados Pessoais

Analisar e aprovar contratos que envolvam tratamento de dados pessoais, seguindo a legislação vigente e aplicável a cada situação em suas particularidades;

Apoiar em sindicâncias para apuração de responsabilidade dos envolvidos em violações de dados pessoais e auxiliar na definição de aplicação das penalidades internas, quando necessário;

Avaliar e auxiliar na elaboração de Relatórios de Impacto à Proteção de Dados Pessoais;

Manter Mapeamento de Fluxos de Dados Pessoais atualizado;

Desenvolver Plano de Análise e Resposta a Violações de Dados Pessoais que identifique o tipo de violação, o número de registros afetados, quais registros foram afetados e as categorias de dados pessoais envolvidas, as notificações apropriadas e plano de mitigação dos efeitos da violação.

Garantir que o tratamento de Dados Pessoais tenha o mesmo nível de tratamento que informações consideradas confidenciais.

8.1.9 Diretoria

Analisar, aprovar e declarar formalmente o seu comprometimento com esta PSI;

Analisar e aprovar, ou não, as exceções de forma excepcional a essa PSI.

9 PENALIDADES

Violações: Qualquer atividade que desrespeite as disposições estabelecidas nesta Norma ou em quaisquer dos documentos complementares da FCAV deve ser considerada como uma violação e tratada pela FCAV a fim de apurar as responsabilidades dos envolvidos de acordo com as “Medidas Disciplinares” da FCAV visando aplicação de sanções cabíveis previstas em cláusulas contratuais e na legislação vigente

Tentativa de Burla: A tentativa de burlar as diretrizes e controles estabelecidos, quando constatada, deve ser tratada como uma violação.

10 DAS DISPOSIÇÕES FINAIS

Esta Política deve ser revisada, no mínimo, anualmente, ou sempre que existir a necessidade de alterações nos critérios definidos nas demais normas e políticas específicas da FCAV.

O presente documento deve ser lido e interpretado sob a égide das leis brasileiras, no idioma português, em conjunto com as normas e procedimentos aplicáveis pela FCAV.

Este documento bem como os demais documentos que a complementam encontram-se disponíveis no ambiente de treinamento da FCAV ou, em caso de indisponibilidade, podem ser solicitados ao Encarregado pelo Tratamento de Dados Pessoais da FCAV.

Qualquer dúvida relativa a esta Política deve ser encaminhada ao Encarregado pelo Tratamento de Dados Pessoais da FCAV por meio do e-mail suportelgpd@vanzolini.org.br .

Esta Política entra em vigor na data de sua publicação.

11 NATUREZA DAS ALTERAÇÕES

Revisão	Alterações (Inclusões ou Exclusões)	Data
0	Emissão Inicial	02/05/2019
1	Harmonização do texto, inclusão do item 5.1d sobre coleta de dados e consentimento, inclusão no item 5.1.4c de responsabilidade específica ao Comitê de Segurança da informação, exclusão do item 13 Vigência da Validade e inclusão do novo item 13 – Natureza das Alterações.	15/05/2020
2	Inclusão da Visão e da Missão no item 1 – Introdução; Inclusão dos objetivos da PSI no item 2 – Escopo; Inclusão do item 3 – Abrangência; Inclusão de referências no item 4; Inclusão de Definições no Item 5 – Definições; Inclusão de Princípios do item 6b; Alteração do texto do item 7 – Requisitos para estabelecer diretrizes e exclusão dos itens: 5.1.4c (da coleta de dados e do consentimento); 6.1.5 (do monitoramento e da auditoria do ambiente), 7 (correio eletrônico); 8 (internet), 9 (identificação), 10 (computadores e recursos tecnológicos), 11 (dispositivos móveis) e 12 (data center/backup). Inclusão de	26/01/2022

	Responsabilidades Específicas no item 8; Inclusão do item 9 – Penalidades; e inclusão do item 10 – Das disposições finais.	

Este plano foi aprovado na Reunião da Diretoria Executiva de 09/02/22