Fundação Escola de Comércio Alvares Penteado

FECAP

POLÍTICA INSTITUCIONAL DE SEGURANÇA DA INFORMAÇÃO_v1

PISI

PORTARIA Nº 495, DE 18 DE JULHO DE 2022 - Ministério da Educação

Departamento de Tecnologia e Informação – Infraestrutura

Outubro de 2024

1. OBJETIVO:

A Política Institucional de Segurança da Informação - PISI tem por objetivo definir e implantar no âmbito da Fundação Escola de Comércio Alvares Peteado (FECAP) o tratamento a ser dado às informações armazenadas, processadas ou transmitidas no ambiente convencional e no ambiente de tecnologia da organização.

A informação utilizada pela escola é um bem de valor e deve ser protegida e gerenciada adequadamente garantindo sua disponibilidade, integridade, confidencialidade, legalidade e auditabilidade, independentemente do meio de armazenamento, processamento ou transmissão adotada.

2. ESCOPO:

A PISI/FECAP abrange os domínios de segurança digital e defesa cibernética, segurança física e proteção de dados organizacionais detendo por escopo ações destinadas à: i) preservação da disponibilidade, integridade, confidencialidade e autenticidade das informações; ii) proteção de dados pessoais e à privacidade, como segue:

a) Diretrizes de comportamentos e procedimentos observados em normas de segurança da informação, comunicação e proteção de dados;
b) Estrutura (física e digital) de gestão de segurança da informação, comunicação e proteção de dados adequada às diretrizes institucionais, considerando o conjunto de papéis, responsabilidades e instrumentos normativos e organizacionais aplicáveis; e
c) Orientações gerais de segurança da informação, comunicação e proteção de dados em harmonia com a legislação vigente, as boas práticas e a gestão eficiente dos riscos associados.

As diretrizes e orientações previstas nesta Política são aplicadas a todos os colaboradores, alunos, professores, terceiros e quaisquer indivíduos da IES (Instituição de Ensino Superior) que tenham acesso às informações, aos dados e aos recursos de Tecnologia da Informação e Comunicação.

3. ARCABOUÇO LEGAL:

. Política Nacional de Cibersegurança e o Comitê Nacional de Cibersegurança:
https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/D11856.htm

. Glossário Segurança da Informação:
https://www.gov.br/gsi/pt-br/ssic/glossario-de-seguranca-da-informacao-1

. Política Corporativa de Segurança da Informação e Proteção de Dados:
https://www.in.gov.br/en/web/dou/-/portaria-n-495-de-18-de-julho-de-2022-416487316

. Lei Geral de Proteção de Dados Pessoais (LGPD):
https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm

. Marco Civil da Internet do Brasil:
https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm

. Lei de acesso à informação: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm

4. CONCEITOS E DEFINIÇÕES:

Ameaça: evento que tem potencial em si próprio para comprometer os objetivos da fundação, seja trazendo danos diretos aos ativos ou prejuízos indiretos decorrentes de situações inesperadas.

Ativos de informação: são os meios de produção, armazenamento, transmissão e processamento de informações, os sistemas de informação, os locais onde se encontram esses meios, as pessoas que têm acesso a informações, assim como as próprias informações coletadas, produzidas, processadas armazenadas, custodiadas, descartadas e transmitidas pela FECAP.

Autenticidade: propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade.

Classificação da informação: identificação de quais são os níveis de proteção que as informações demandam e estabelecimento de classes e formas de identificá-las, além de determinar os controles de proteção necessários a cada uma delas.

Confidencialidade: propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizados e credenciados.

Conformidade: processo que visa verificar o cumprimento das normas estabelecidas. **Controle de acesso**: conjunto de procedimentos recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso.

Criptografia: método de codificação da informação que visa evitar que ela seja compreendida ou alterada por pessoas não autorizadas. Anonimização.

Dados pessoais: todo e qualquer dado relacionado a pessoa natural identificada ou identificável (conforme definição trazida no art. 5 0, I, da Lei n o 13.709/2018 — Lei Geral de Proteção de Dados Pessoais), inclusive números identificativos, dados locacionais ou identificadores eletrônicos/ quando estes estiverem relacionados a uma pessoa. Também são considerados dados pessoais para os fins da lei aqueles utilizados para formação do perfil comportamental de determinada pessoa natural se identificada (art. 12, 52 0, LGPD).

Disponibilidade: propriedade de que a informação esteja acessível e utilizável, sob demanda, por uma pessoa física ou determinado sistema, órgão ou entidade no momento requerido.

Fornecedores: terceiros contratados e subcontratados, pessoa física ou jurídica.

Informação: conjunto de dados, textos, imagens, métodos, sistemas ou quaisquer formas de representação dotadas de significado em determinado contexto, independentemente do suporte em que resida ou da forma pela qual seja veiculado.

Infraestrutura de tecnologia da informação: instalações prediais (energia, água, climatização/ acesso físico), computadores e equipamentos, software, redes e telecomunicações, sistemas de armazenamento e recuperação de dados (arquivos e armazenamento) aplicações computacionais, cabeamento e rede telefônica.

Integridade: propriedade de que a informação não foi modificada, suprimida ou destruída de maneira não autorizada ou acidental.

Lei geral de proteção de dados pessoais (LGPD): Lei no 13.709/2018, que dispõe sobre o tratamento de dados pessoais, em meios físicos ou digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade, nos termos da Lei (Arts. 10 e 17 LGPD).

Parceiros comerciais: terceiros contratados pessoa física ou jurídica, que atuam em nome da escola: Consultores, Conveniados e Agentes Comerciais.

Quebra de segurança: ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação e das comunicações.

Segurança de comunicações: processo de proteção de dados digitais em trânsito.

Sistema estruturante: conjunto de sistemas de informática fundamentais e imprescindíveis para a consecução das atividades administrativas, de forma eficaz e eficiente.

Terceiros: São os parceiros comerciais e os fornecedores da FECAP.

Tratamento da informação: conjunto de ações referentes à recepção, produção, reprodução, utilização, acesso, transporte, transmissão, distribuição, armazenamento, eliminação e controle da informação.
Vulnerabilidade: fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças.

Para os devidos fins esta política acata e considera ainda o **Glossário de Segurança da Informação**[1] da Secretaria de Segurança da Informação e Cibernética da União (Gabinete de Segurança Institucional).

5. PAPÉIS E RESPONSABILIDADES:

A Política Institucional de Segurança da Informação da FECAP descreve os seguintes papéis e responsabilidades:

a) Administradores de recursos de Tecnologia da Informação e Comunicações: equipe técnica (DTI Infra) responsável por um sistema de processamento de informações, serviço ou infraestrutura de TIC;

b) Custodiante da informação (qualquer pessoa que detém a posse das informações e dos dados): responsável por garantir a segurança das informações e dos dados sob sua posse e comunicar sobre situações que comprometam essa garantia;

c) Gestor da informação (colegiado, autoridade ou dirigente): responsável por classificar as informações e os dados sob sua gestão e definir procedimentos e critérios de acesso;

d) Proprietário do ativo de informação: refere-se à parte interessada, pessoa natural ou jurídica, de direito público ou privado. Indivíduo legalmente instituído por sua posição e/ou cargo, o qual é responsável primário pela viabilidade e sobrevivência dos ativos de informação; e

e) Usuário de informação (ou usuário): pessoa física, seja colaborador seja equiparado, empregado ou prestador de serviços, habilitada pela Administração para acessar os ativos de informação na escola, formalizada por meio da assinatura de termo de responsabilidade. 6. PRINCÍPIOS:

As ações de segurança da informação, comunicações e proteção de dados da FECAP têm como premissa as definições contidas na Política Nacional de Segurança da Informação - PNSI[2], mas não somente, assim os princípios orientadores também se fazem presentes:

a) **Alinhamento estratégico e sistêmico**: Política Institucional de Segurança da Informação com o planejamento estratégico institucional (PDI), com o modelo de governança e com a Gestão de Riscos e Controles Internos (*Compliance*) pertinentes;

b) **Universalidade e uniformidade**: abrangência gradual e permanente a todos os processos organizacionais observando os mesmos conceitos, referenciais técnicos e procedimentos em todos os níveis corporativos da escola;

c) **Transparência**: obrigação fundamental de prestar informações confiáveis, relevantes aos usuários dos ativos da informação garantindo seu sigilo e inviolabilidade da intimidade da vida privada, da honra e da imagem das pessoas;

[1] Portaria GSI/PR Nº 93, DE 18 DE Outubro DE 2021: https://www.gov.br/gsi/pt-br/ssic/glossario-deseguranca-da-informacao-1
[2] https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/D9637.htm

d) **Corresponsabilidade**: constituída pelo dever de todas as partes envolvidas em conhecer e respeitar a Política Institucional de Segurança da Informação da IES;

e) **Continuidade dos processos e serviços críticos**: essenciais ao funcionamento e ao cumprimento de sua missão institucional (protegendo sua disponibilidade e segurança e definindo estratégias de prevenção, gestão e recuperação de incidentes, política de becape e restauração de dados, visando à continuidade do negócio e à redução de interrupções); e

f) **Educação, comunicação e cooperação**: para fomento e aprimoramento das práticas de promoção da cultura em segurança da informação e perenidade dos mecanismos relacionados.

7. DIRETRIZES:

A gestão de segurança da informação é suportada por ações e métodos que visem à integração das atividades de gestão de riscos, à gestão de continuidade do negócio, ao tratamento de incidentes, segurança cibernética e conformidade regulatória.

a) Informações e dados como ativos: toda e qualquer informação e dado gerados, custodiados, manipulados, utilizados ou armazenados junto a IES compõem o ativo de informação relevante para as suas atividades e devem ser protegidos e tratados com vistas à preservação dos princípios de disponibilidade, integridade, confidencialidade e autenticidade bem como à proteção de dados pessoais e à privacidade;

b) Classificação da informação como requisito: todo ativo de informação deve ser classificado e tratado segundo sua classificação de segurança da informação, de maneira a proteger adequadamente as informações e os dados;

c) Segregação de funções: sempre que processualmente viável, devem ser segregadas funções ou áreas de responsabilidade conflitantes, para que ninguém detenha controle de um processo crítico na sua totalidade;

d) Estabelecer controles adequados ao risco: as medidas e os controles de segurança devem ser estabelecidos considerando a relevância dos ativos de informação e os níveis de risco associados, visando sempre à prevenção da ocorrência de incidentes;

e) Menor privilégio e mínimo acesso: pessoas e aplicações devem ter o menor privilégio e o mínimo de acesso aos recursos necessários para realizar uma determinada tarefa;

f) Responsabilização individual: todos os usuários são responsáveis pela segurança dos ativos de informação que estejam sob sua custódia, pelo uso e pela guarda de suas credenciais de acesso, sendo vedada a exploração de eventuais vulnerabilidades;

g) Corresponsabilidade de terceiros: todos os contratos de prestação de serviços, firmados pela escola deverão conter cláusula específica sobre a obrigatoriedade de atendimento às diretrizes desta política e, ou à Política de Privacidade e Proteção de Dados Pessoais da escola;

h) Restrição de uso dos ativos de informação: o acesso e uso das informações e dados que não sejam de domínio público e dos ativos de informação são controlados e limitados às atribuições necessárias para cumprimento das atividades dos solicitantes apenas para as finalidades profissionais, lícitas e éticas;

i) Uso seguro dos ativos de informação: apenas os ativos de informação homologados e autorizados pela FECAP devem ter uso permitido, desde que sejam identificados de forma individual, protegidos e tenham um proprietário do ativo de informação responsável.

Essas diretrizes gerais constituem os pilares da gestão de segurança da informação e proteção de dados da FECAP e norteiam ações, planos e normas associados com vistas a garantia dos princípios de segurança da informação estabelecidos neste instrumento.

8. TRATAMENTO DA INFORMAÇÃO:

Toda informação e dado criados manuseados, armazenados, transportados, descartados devem ser classificados e tratados adequadamente, quanto aos aspectos de confidencialidade, integridade, autenticidade e disponibilidade bem como à proteção de dados pessoais e à privacidade, de forma explícita ou implícita, em harmonia com as legislações aplicáveis.

Toda informação e dado institucionais, se eletrônicos, serão armazenados nos servidores de arquivos e bases de dados sob gestão e administração da FECAP e, se não eletrônicos, mantidos em local físico adequado.
No descarte de informações e dados institucionais, deverão ser observadas - além das próprias métricas institucionais setoriais, a legislação vigente, em especial às definições da Lei nº 12.527, de 2011 e as **tabelas de temporalidade governamentais**[3].

Ao aplicar uma classificação a um documento e/ou informação/dado, todos os agentes responsáveis devem usar o bom senso, adotando como princípio orientador a garantia do direito de acesso à informação.

Os agentes responsáveis pelo tratamento dos dados são responsáveis por (**i**) decidir a classificação das informações e dos dados relevantes, (**ii**) comunicar o valor e a classificação da informação, e (**iii**) controlar o acesso às informações e aos dados custodiados. O usuário de informação, por sua vez, é responsável pela proteção da segurança e integridade das informações e dos dados em sua posse (acesso), devendo se familiarizar com as normas específicas do custodiante (FECAP).

9. CONTROLES DE ACESSO:

Todo usuário de informação que faça uso dos recursos de Tecnologia da Informação e Comunicação deverá possuir credenciais de acesso único e intransferível, que permitam seu reconhecimento individual inequívoco, com gerenciamento regulamentados e consoantes a esta política.

A concessão e a revogação dos privilégios de acesso às informações ficam atribuídas ao agente responsável pelo tratamento dos dados sob a sua tutela, considerando sempre o "**princípio do menor privilégio**[4]".

9.1 SEGURANÇA FÍSICA DO AMBIENTE:

As ações de segurança física e ambiental, no que se referem aos aspectos de segurança da informação, proverão:

a) Controle e monitoramento de acesso físico: compreendem as necessidades de controle e monitoramento e registro de acesso às instalações e aos ambientes físicos de tecnologia da escola;

b) Controles ambientais: compreendem provisão e manutenção dos controles ambientais necessários, com base em uma avaliação de requisitos, que inclui, mas não se limita, a

[3] https://www.gov.br/arquivonacional/pt-br/servicos/gestao-de-documentos/orientacao-tecnica-1/codigo-de-classificacao-e-tabela-de-temporalidade-e-destinacao-de-documentos-de-arquivo

[4] https://www.gov.br/gsi/pt-br/ssic/osic/OSIC%2009.23

energia de reserva para facilitar um processo de desligamento ordenado (no mínimo) e monitoramento de temperatura e umidade;

10. GESTÃO DE INCIDENTES EM SEGURANÇA DA INFORMAÇÃO:

Provisão de normas e procedimentos de resposta a incidentes consistentes com as leis e políticas governamentais aplicáveis, incluindo, mas não se limitando, a identificação de papéis e responsabilidades, a investigação, os procedimentos de contenção e escalonamento, a documentação e preservação de evidências, os protocolos de comunicação e as lições aprendidas.

O processo de gestão de incidentes deverá envolver também métricas estabelecidas pela Biblioteca de Infraestrutura de Tecnologia da Informação (**ITILv4**[5]) procedimentos adequados de comunicação de incidentes incluindo, mas não se limitando ao treinamento de colaboradores e terceiros para identificar e comunicar rapidamente incidentes e preparação e apresentação de relatórios de acompanhamento.

10.1 GESTÃO DE ATIVOS:

A FECAP manterá um processo de inventário e mapeamento dos ativos de informação objetivando a segurança das estruturas críticas que garantem suas informações e dados. O processo de inventário e mapeamento de ativos de informação subsidiará o conhecimento, a valoração, a proteção e a manutenção de seus ativos de informação e deverá ser dinâmico, periódico e estruturado, para manter a base de dados de ativos de informação atualizada.

10.2 GESTÃO DE COMUNICAÇÕES – CORREIO ELETRÔNICO (E-MAIL):

Todos os sistemas de comunicação eletrônica, quer seja de origem externa quer seja interna, deverão ser utilizados precipuamente no exercício das funções institucionais, em conexão com a finalidade da escola, de forma aderente a esta Política e à legislação vigente. Podendo, portanto, ser concedidos ou revogados a qualquer tempo, em caráter total ou parcial, de acordo com os interesses da FECAP.

A IES se reserva o direito de monitorar, acessar e revisar quaisquer aspectos de seus recursos de informação eletrônica e sistemas de comunicação, incluindo, entre outros, o uso da internet, sistemas de comunicação eletrônica (e-mails), sistemas de telefonia, tráfego da rede e revisar ativos armazenados em qualquer sistema de comunicação. **O consentimento para tais registros e monitoramento é presumido por parte dos usuários, não cabendo qualquer contestação ou alegação de desconhecimento dessa regra.**

As comunicações eletrônicas são comunicações formais e espera-se que os usuários exerçam cuidado e profissionalismo na aplicação desses recursos, assim como o faria com qualquer outro expediente de comunicação formal emitido em nome da FECAP.

11. ACESSO À INTERNET:

O acesso à internet no ambiente de trabalho está condicionado às necessidades dos indivíduos (colaboradores, professores, no exercício de suas atribuições e será regido por norma específica, em conformidade com esta PISI/FECAP e demais orientações, normativas e legislação em vigor.

Cada usuário de informação é responsável por tomar todas as medidas razoáveis para utilizar os recursos de internet de forma responsável e segura (credenciais de acesso são pessoais e

[5] https://www.itlibrary.org/

intransferíveis, sendo que o usuário é individualmente responsável por todas as atividades exercidas a partir de sua credencial).

No que se refere ao acesso à internet, cada usuário deverá:

a) Utilizar os recursos de forma a proteger a organização de qualquer risco legal, regulatório, operacional ou de reputação;

b) Não compartilhar suas credenciais de acesso;

c) Não acessar websites ou objetos com conteúdo inadequado ou ilegal;

d) Estar ciente de suas responsabilidades pelo uso apropriado da internet e de que o uso dela está sujeito a registro e pode ser monitorado de acordo com as exigências das leis e dos regulamentos aplicáveis. 11.1 COMPUTAÇÃO EM NUVEM:

O uso de serviços em nuvem deverá assegurar que toda a cadeia de suprimentos de TIC baseada em provedores de serviços no ambiente de computação em nuvem seja avaliada e pautada à proteção de dados, metadados, informações e conhecimentos produzidos ou custodiados pela instituição, incluindo o cumprimento da legislação e regulamentação incidentes, gerenciamento de identidades (acesso credenciado), o monitoramento e auditorias pertinentes.

12. DESENVOLVIMENTO SEGURO DE SOFTWARE:

O processo de desenvolvimento de software prioriza a adoção de práticas voltadas à segurança da informação como modelagem de ameaças, análise estática do código, revisão de código, testes de segurança direcionados (ambientes de desenvolvimento e homologação segmentados) objetivando a minimização de vulnerabilidades e menor impacto ao ambiente de produção.
A segurança da informação delimitará a lista de requisitos, desde a concepção dos projetos de desenvolvimento e/ou aquisição de software (**“Privacy by Design” e “Privacy by Default”**[6]).

13 AUDITORIA E CONFORMIDADE:

O uso dos recursos de Tecnologia da Informação e Comunicação dispostos pela IES é passível de monitoramento e auditoria (incluindo a análise regular de registros de eventos [log] com aplicação, sempre que viável, de softwares utilitários específicos para monitoramento do uso de sistemas computacionais.

Sempre que possível, deverão ser implementados e mantidos mecanismos que permitam a rastreabilidade dos recursos de TIC por meio de estratégias como: trilhas de auditoria, rastreamento, acompanhamento, controle e verificação de acessos para todos os sistemas corporativos e rede corporativa.

Como medida de preservação de evidências, **sempre que tecnicamente possível**, todo e qualquer ativo de informação deverá ser configurado para armazenar registros históricos de eventos [log] em formato que permita a completa identificação dos fluxos de dados e das operações de seus usuários e/ou administradores. Esses registros devem ser armazenados pelo período mínimo de seis meses, sem prejuízo à operação do recurso e os serviços servidos. 14. PENALIDADES:

Ações que violem a Política Institucional de Segurança da Informação – PISI, caracterizam infração funcional e poderão acarretar, isolada ou cumulativamente sanções administrativas respeitando a seguinte hierarquia: a) liderança local e ou imediata; b) Recursos Humanos/Jurídico, e; c) Reitoria, assegurado aos envolvidos o contraditório e a ampla defesa.

15. ATUALIZAÇÃO E REVISÃO:

A Política Institucional de Segurança da Informação - PISI será revisada e atualizada em função de alterações na legislação pertinente, das diretrizes do Ministério da Educação e Cultura (MEC), de alterações nos normativos pertinentes quando considerados necessários e aprovados pela Reitoria da IES no prazo máximo de um ano a contar da data de sua publicação. 16. CLASSIFICAÇÃO DAS INFORMAÇÕES:

As informações e os dados da escola requerem classificação para otimizar os controles que garantam seu acesso por pessoas autorizadas, portanto, afastando incidentes de dados e garantindo os princípios de Autenticidade e Confidencialidade previstos junto a Norma ABNT NBR ISO/IEC 27001[6].

A Classificação da Informação institucional é amplamente discutida junto ao **ANEXO I**.

As diretrizes que regem a utilização de senhas da IES são abordadas junto ao **ANEXO II**

DISPOSIÇÕES FINAIS:

Esta Política Institucional de Segurança da Informação - PISI é pública e suas atualizações deverão ser divulgadas amplamente a todos os indivíduos com vínculo estabelecido com a IES, ainda que sua atuação seja temporária.

É responsabilidade de todos os gestores da FECAP promover o conhecimento e a disseminação desta Política e demais normas associadas à segurança da informação aos colaboradores e demais pessoas e terceiros sob a sua gestão.

[6] https://www.abntcatalogo.com.br/pnm.aspx?Q=WXV0VDkwSGkvd0dKUVRPMVpjcTR1VUJDS2FvZ21LUnNURUVsamtWT0xIbz0=

ANEXO I – CLASSIFICAÇÃO DA INFORMAÇÃO[7]

A classificação de toda informação da Fundação Escola de Comércio Alvares Penteado – FECAP, cumpre acordo à Lei de Acesso à Informação (12.527/2011) que tipifica e regimenta este conteúdo e acesso.

Justifica-se tal acato diante do artigo 2 da referida legislação, 12.527/2011:

> "*Aplicam-se as disposições desta Lei, no que couber, às entidades privadas sem fins lucrativos que recebam, para realização de ações de interesse público, recursos públicos diretamente do orçamento ou mediante subvenções sociais, contrato de gestão, termo de parceria, convênios, acordo, ajustes ou outros instrumentos congêneres*."

Portanto, para os respectivos efeitos, consideram-se:

a) **Informação**: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;
b) **Documento**: unidade de registro de informações, qualquer que seja o suporte ou formato;
c) **Informação** sigilosa: aquela submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado;
d) **Informação pessoal**: aquela relacionada à pessoa natural identificada ou identificável;
e) **Tratamento da informação**: conjunto de ações referentes à produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle da informação;
f) **Disponibilidade**: qualidade da informação que pode ser conhecida e utilizada por indivíduos, equipamentos ou sistemas autorizados;
g) **Autenticidade**: qualidade da informação que tenha sido produzida, expedida, recebida ou modificada por determinado indivíduo, equipamento ou sistema;
h) **Integridade**: qualidade da informação não modificada, inclusive quanto à origem, trânsito e destino;
i) **Primariedade**: qualidade da informação coletada na fonte, com o máximo de detalhamento possível, sem modificações.

Não obstante a Lei Geral de Proteção de Dados Pessoais do Brasil (LGPD) Nº 13.709, de 14 de agosto de 2018 em seu artigo 5º, para os fins desta política, considera:

. dado pessoal: informação relacionada a pessoa natural identificada ou identificável;
. dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;
. 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.

Diante do apresentado, o acesso à informação compreende, entre outros, os direitos de obter:

. orientação sobre os procedimentos para a consecução de acesso, bem como sobre o local onde poderá ser encontrada ou obtida a informação almejada;

. informação produzida ou custodiada por e para pessoa física ou entidade privada decorrente de qualquer vínculo com seus órgãos ou entidades, mesmo que esse vínculo já tenha cessado;

[7] Reis, B., Mota, J. C., & de Oliveira, P. P. B. Classificação da Informação. https://www.lyfreitas.com.br/ant/artigos_mba/artclassinfo.pdf. Acesso em 22 de janeiro de 2024.

. informação primária, íntegra, autêntica e atualizada;

. informação sobre atividades exercidas pela escola, inclusive as relativas à sua política, organização e serviços;

Dado o preâmbulo jurídico preconizado, dispõe-se uma escala de quatro níveis de sensibilidade da informação institucional:

Nível 1 – Informação **pública** ou **aberta**: informação que foi obtida sem ônus, de fontes públicas, ou que foi produzida internamente pela empresa sob interesse público. Essas informações não precisam de controle de acesso e de distribuição. Apenas deve-se assegurar que elas não sejam danificadas ou adulteradas.

São exemplos de informações de nível 1: Dados do balanço de empresas de capital aberto; Lista de produtos e serviços; Notícias sobre a empresa.

Nível 2 – Informação **interna** ou **operacional**: A informação deve ser classificada como interna quando não for desejável que ela se torne conhecida de fora da organização. Contudo, face a um eventual vazamento em que se torne pública, o prejuízo (impacto) a instituição é baixa ou ausente. Como são informações relevantes ao funcionamento dos negócios, precisam principalmente ter sua integridade protegida e incidentes, internos ou externos, relatados às autoridades competentes, e.g. ANPD[8].

São exemplos de informações de nível 2: Relatórios de consultoria sobre empresas concorrentes; Dados pessoais dos funcionários e executivos da empresa; Relatos de defeitos de produtos e serviços. Contratos e parceiras de negócio(s).

Nível 3 – Informação **confidencial** ou **sigilosa**. A informação classifica-se como confidencial quando sua exposição fora do ambiente organizacional pode gerar perdas financeiras, de imagem, de competitividade etc. Para proteção de uma informação confidencial, se faz necessário, além de controles de acesso, mecanismos que garantam sua integridade, pois são informações imperativas às atividades da escola. Recomenda-se evitar transmissão de informações confidenciais, via Internet sem o uso de criptografia ou métodos que garantam sua anonimização ou pseudoanonimização, minimamente.

São exemplos de informações de nível 3: Relatórios de investigação de práticas concorrenciais ilegais; Detalhes sobre campanhas de lançamento comercial; Detalhes sobre planos de fusão, aquisição ou fechamento de empresas. Relatórios médicos e, ou psicológicos de colaboradores e, ou estudantes.

Nível 4 – Informação **restrita** ou **secreta**. A informação deve ser classificada como restrita quando acessos não autorizados a ela, mesmo que por membros da própria organização, sejam capazes de trazer sérios danos ao negócio. Logo, a informação restrita precisa ser protegida contra acessos internos e externos. São ainda mais importantes que as informações confidenciais e por isso devem receber um grau de proteção ainda mais elevado.
Só devem ter acesso a informações restritas pessoas que necessitem dessas informações para a realização de suas atividades, independentemente do cargo ocupado.

[8] https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/comunicado-de-incidentede-seguranca-cis

São exemplos de informações de nível 4: Detalhes de produtos e serviços em desenvolvimento; Detalhes de negociação de compra ou venda de empresas ou filiais; Relatórios sobre falhas graves, em produtos, serviços ou processos internos; Relatórios de acesso indevido a internet, investigações junto aos sistemas de câmeras internas da escola (CFTV). Planos de demissão. Dados sensíveis de pessoas naturais com vínculo com a escola (colaboradores, professores ou alunos).

A segmentação das informações em níveis de sensibilidade permite que sejam planejados esforços de proteção adequados, reduzindo riscos e permitindo a atribuição de responsabilidades às pessoas, de tal forma, a delinear estratégias (níveis de segurança) alinhados com a referida sensibilidade:

Irrestrito – A informação é pública, podendo ser utilizada por todos sem causar danos à organização;
Interna – A informação é interna, aquela que a organização não tem interesse em divulgar, cujo acesso por parte de indivíduos externos evita-se, ainda assim, face a disponibilização indevida os danos (impactos) são baixos ou ausentes;
Confidencial – Informação confidencial da organização cuja divulgação pode causar danos financeiros ou à imagem da organização. Essa divulgação pode gerar vantagens a eventuais concorrentes e perda de clientes;
Secreta – Informação restrita a um grupo seleto dentro da organização. Sua integridade deve ser preservada a qualquer custo e o acesso rigidamente limitado e seguro. Informação considerada vital para a instituições.

Resposta de Segurança para **armazenamento** de informações:

Sensibilidade informação	Nível de segurança	Impressos	Digitais
Pública	Irrestrito	Sem requisitos especiais	Backups regulares
Interna	Protegido	Guardado em local seguro	Armazenado em áreas restritas da LAN
Confidencial	Confidencial	Local seguro com acesso restrito	Armazenado em áreas restritas da LAN com acesso limitado
Restrita	Secreto	Local seguro com controle de acesso	Armazenado em áreas restritas da LAN com senha (forte), encriptado e trilhas de auditoria aplicadas.

Resposta de Segurança para transmissão de informações:

Sensibilidade informação	Nível de segurança	Impressos	Digitais
Pública	Irrestrito	Sem requisitos especiais	Sem requisitos especiais
Interna	Protegido	Envelopes lacrados ou cartas registradas	Criptografia e, ou senha em arquivos transmitidos
Confidencial	Confidencial	Envelope lacrado com carimbo “confidencial” e notificação de recebimento	Criptografia ou senhas em arquivos transmitidos utilizando VPN e confirmação de recebimento
Restrita	Secreta	Envelope com duplo lacre transportado sob custódia	Tratamento anterior acrescido de auditoria de processo (mail delivery)

Aplicam-se a este anexo, Classificação da Informação, as disposições finais da Política Institucional de Segurança da Informação (PISI), observáveis junto ao item 17, página 8.

ANEXO II – POLÍTICA DE SENHAS INSTITUCIONAIS

1. OBJETIVO:

Esta política pretende aumentar a garantia da segurança das informações institucionais por meio da implementação de práticas rigidas de gerenciamento de senhas, conforme as diretrizes preconizadas pelo Center for Internet Security (CIS)[9] e National Institute of Standards and Technology (NIST)[10].

2. ESCOPO:

Aplica-se a todos os funcionários, contratados e terceiros (indivíduos de natureza privado ou pública, titulares de dados) que tenham acesso aos sistemas e dados da empresa.

3. REQUISITOS DE SENHAS:

. Comprimento Mínimo: As senhas devem ter no mínimo 14 caracteres.
. Complexidade: As senhas devem incluir uma combinação de letras maiúsculas e minúsculas, números e caracteres especiais.
. Proibições: Não são permitidos nomes do titular, caracteres repetitivos ou sequenciais (por exemplo, ‘aaaaaa’, ‘123456’).

4. RENOVAÇÃO DE SENHAS:

. Periodicidade máxima: As senhas devem ser alteradas a cada 60 dias máximos;
. Periodicidade mínima: As senhas poderão ser alteradas após 1 dia da última alteração;
. Histórico de Senhas: Não é permitido reutilizar as últimas 6 senhas (12 meses).

5. BLOQUEIO DE CREDENCIAIS:

. As credenciais de acesso serão bloqueadas após 5 (cinco) tentativas sem sucesso;
. O bloqueio permanecerá por 10 minutos;

6. AUTENTICAÇÃO MULTIFATOR (MFA):

Implementação: MFA deve ser habilitada sempre que possível para todos os acessos a sistemas institucionais.

7. EDUCAÇÃO E CONSCIENTIZAÇÃO:

Treinamento: Todos os funcionários devem receber treinamento regular sobre a importância da segurança das senhas e práticas recomendadas.

8. MONITORAMENTO E AUDITORIA:

Monitoramento Contínuo: Implementar sistemas de monitoramento para detectar tentativas de acesso não autorizadas.
Auditorias Regulares: Realizar auditorias periódicas para garantir a conformidade com a política de senhas.

[9] https://www.cisecurity.org/insights/white-papers/cis-password-policy-guide
[10] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf

9. RESPONSABILIDADES:

Usuários: Devem criar senhas que atendam aos requisitos e mantê-las confidenciais.
Equipe de TI: Responsável por implementar e monitorar a conformidade com esta política.