POLÍTICAS E NORMAS COMPLEMENTARES

- Política de Segurança de Informação e Privacidade

Política de Segurança de Informação e Privacidade

Introdução

Este documento define a política de segurança da informação e privacidade do Projeto SciELO/FapUnifesp com o objetivo de proteger as fontes de informação de sua propriedade, sob sua responsabilidade ou em seu uso, que são utilizadas na gestão e operação de seus produtos e serviços. A política se aplica a todos os colaboradores do projeto, aos parceiros, usuários e apoiadores. Ela é referida doravante como PSI.

A PSI é definida e gerida pela direção do Projeto SciELO/FAPESP. Ela orienta o funcionamento e atualização do Sistema de Gestão de Segurança da Informação do Projeto SciELO/FapUnifesp, com as seguintes funções que objetivam assegurar a continuidade dos processos e qualidade dos seus produtos e serviços:

1. Garantir a integridade, disponibilidade e, quando se aplicar, a confidencialidade das fontes de informação de propriedade Projeto SciELO/FapUnifesp, sob sua responsabilidade ou em seu uso;
2. Garantir o atendimento à legislação vigente e requisitos contratuais;
3. Promover a capacitação de seus colaboradores;
4. Promover a melhoria contínua do Sistema de Gestão da Segurança da Informação.

Abrangência

A PSI aplica-se a todos os colaboradores e terceiros que utilizem as fontes de informação de propriedade do SciELO/FapUnifesp ou operadas sob sua responsabilidade.

Legislação Aplicável

Correlacionam-se com a PSI e sua aplicação as leis abaixo relacionadas, mas não limitadas às mesmas:

1. Lei Federal 8159, de 08 de janeiro de 1991 (Dispõe sobre a Política Nacional de Arquivos Públicos e Privados)
2. Lei Federal 9610, de 19 de fevereiro de 1998 (Dispõe sobre o Direito Autoral)
3. Lei Federal 9279, de 14 de maio de 1996 (Dispõe sobre Marcas e Patentes)
4. Lei Federal 3129, de 14 de outubro de 1982 (Regula a Concessão de Patentes aos autores de invenção ou descoberta industrial)
5. Lei Federal 10406, de 10 de janeiro de 2002 (Institui o Código Civil)
6. Decreto-Lei 2848, de 7 de dezembro de 1940 (Institui o Código Penal)
7. Lei Federal 9983, de 14 de julho de 2000 (Altera o Decreto-Lei 2.848, de 7 de dezembro de 1940 – Código Penal e dá outras providências)
8. Lei Federal 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais (LGPD)

Informação Documentada – Estrutura Normativa

Os documentos que compõem a estrutura normativa da PSI são divididos em categorias:

1. Política/ Normas / Diretrizes (nível estratégico): Contidas neste documento, definem as regras de alto nível de segurança da informação que o Projeto SciELO/FapUnifesp incorpora à sua gestão de acordo com sua estratégia programática. Servem de base para que os procedimentos sejam criados e detalhados;
2. Processos / Procedimentos (nível operacional): Instrumentalizam o disposto na PSI, permitindo a direta aplicação nas atividades do Projeto SciELO/FapUnifesp;
3. Guias (nível operacional);
4. Templates (nível operacional).

Todos os documentos são disponibilizados por meio do Portal do Sistema de Gestão de Segurança da Informação do Projeto SciELO/FapUnifesp e depositados em seus repositórios de documentos. Novos documentos ou revisões devem ser aprovadas pelos gestores das áreas responsáveis antes de serem disponibilizados.

Cópias impressas de conteúdos do Portal do Sistema de Gestão de Segurança da Informação não são consideradas válidas e são proibidas.

Os documentos integrantes da estrutura são divulgados a todos os colaboradores, estagiários, aprendizes e prestadores de serviços do Projeto SciELO/FapUnifesp quando de sua admissão, bem como, por seus meios oficiais de divulgação interna e, também, publicadas no Portal do Sistema de Gestão de Segurança da Informação, de maneira que seu conteúdo possa ser consultado a

qualquer momento.

Toda alteração realizada na PSI deverá ser repassada ao Diretor do Programa SciELO, responsável pelo Projeto SciELO/FapUnifesp, para aprovação e, após aprovação, divulgada na nova baseline organizacional.

Classificação das fontes de Informação

As fontes de informação e informação que delas se derivam, que são de propriedade do Projeto SciELO/FapUnifesp ou que estão sob sua custódia, são classificadas de maneira proporcional ao seu valor e impactos na estratégia e negócios para o SciELO/FapUnifesp.

A informação abarcada pela PSI deve ser classificada conforme a Norma de Classificação e Manuseio da Informação (NCMI).

Os acessos à informação são controlados por níveis de permissão conforme as definições da Norma de Controle de Acessos, limitando o acesso apenas às pessoas autorizadas em sistemas ou pastas de arquivos.

As seguintes regras se aplicam no tratamento da informação de acordo com seu nível de classificação:

1. Fonte de informação sem um rótulo de nível de classificação deve ser considerada por padrão como nível Pública;
2. É obrigatório rotular todas as fontes de informação de nível Confidencial (documentos, planilhas e outros arquivos);
3. Quando necessária a impressão, documentos Confidenciais ou Internos devem ser impressos apenas em impressoras localizadas em salas de acesso restrito e retiradas imediatamente pelos responsáveis;
4. Deve-se evitar o envio de documentos Confidenciais por e-mail, porém caso seja necessário deve-se utilizar algum tipo de criptografia no documento ou na mensagem;
5. Caso tenha acesso a uma fonte de informação ou informação confidencial, privada ou interna (conforme a NCMI) fora do seu escopo de trabalho, comunique imediatamente a Unidade de Infraestrutura do Projeto SciELO/FapUnifesp. Se for um documento devolver ao responsável ou à Infraestrutura.

Competências Necessárias para Segurança da Informação

As pessoas responsáveis pela gestão do SGSI devem possuir competências necessárias para desempenhar suas funções de forma adequada e garantir assim o sucesso do SGSI. As competências exigidas devem:

1. Estar formalmente previstas mediante justificativa que demonstre a devida compatibilidade com o SGSI baseado na ISO 27001:2013;
2. Deve possibilitar que as pessoas sejam competentes com base na educação, treinamento ou experiência apropriadas;
3. Reter informação documentada adequadamente, como prova de competência.

Diretrizes de Segurança da Informação

A PSI define as seguintes diretrizes que norteiam as atividades profissionais de cada colaborador, estagiário, aprendiz ou prestador de serviços do Projeto SciELO/FapUnifesp:

1. Os colaboradores devem assumir uma postura proativa de proteção das fontes de informação de propriedade ou sob responsabilidade do Projeto SciELO/FapUnifesp e de informação delas derivada, que compreende, entre outros posicionamentos, estar atentos a ameaças externas, fraudes, roubos e acesso indevido;
2. Assuntos confidenciais não devem ser expostos publicamente;
3. Senhas, chaves e outros recursos de caráter pessoal são considerados intransferíveis e não podem ser compartilhados e divulgados;
4. Somente softwares homologados, podem ser utilizados no ambiente computacional do Projeto SciELO/FapUnifesp;
5. Fontes de informação confidenciais (documentos impressos, arquivos, sistemas) devem ser armazenados apropriadamente e protegidos. O descarte deve ser feito respeitando o procedimento de descarte conforme as definições da Norma de Classificação e Manuseio de Informação;

6. Todas as fontes de informação e qualquer informação delas derivada que são considerados imprescindíveis ao desenvolvimento e operação do Projeto SciELO/FapUnifesp devem ser protegidas por meio de rotinas sistemáticas e documentadas de cópia de segurança, devendo ser submetidos a testes periódicos de recuperação;
7. O acesso às dependências do Projeto SciELO/FapUnifesp deve ser controlado e assegurada e integridade, disponibilidade e, quando se aplica, a confidencialidade das fontes de informação ali armazenadas ou operadas de modo a garantir a rastreabilidade e efetividade dos acessos autorizados;
8. O acesso via sistemas computacionais disponibilizados pelo Projeto SciELO/FapUnifesp devem ser controlados e assegurada a integridade, disponibilidade e, quando se aplica, a confidencialidade das fontes de informação da informação de modo a garantir a rastreabilidade e a efetividade dos acessos autorizados.
9. São de propriedade do Projeto SciELO/FapUnifesp todas as criações, códigos ou procedimentos desenvolvidos por qualquer colaborador, estagiário, aprendiz ou prestador de serviço durante o curso de seu vínculo com o Projeto.

Avaliar Riscos à Segurança da Informação

Os riscos à segurança das fontes de informação do Projeto SciELO/FapUnifesp são identificados seguidamente por meio de mapeamento de vulnerabilidades, ameaças, impacto e probabilidade de ocorrência e de controles que mitigam estes riscos junto dos donos de riscos responsáveis. Duas instâncias são sistematicamente mapeadas e controladas: o ambiente físico e atuação de fornecedores.

1. Ambiente físico

O acesso aos ambientes físicos do Projeto SciELO/FapUnifesp deve ser controlado e monitorado. Acesso a ambientes críticos deve ter o acesso restrito conforme declaração na Norma de Controle de Acessos.

2. Fornecedores

Fornecedores, que podem ter acesso a fontes de informação confidenciais e a dados pessoais, devem possuir cláusulas de segurança e sigilo de informação em seus contratos. Os fornecedores devem ser avaliados quanto ao nível de segurança, conforme os requisitos estabelecidos nesta política, quanto à gestão de acesso, análise de vulnerabilidades e continuidade de negócios e devem possuir em seus contratos SLA estabelecido.

Compartilhamento

O compartilhamento de fontes de informação não é permitido em equipamentos pessoais. Todas as fontes de informação devem ser armazenadas em servidores das redes do Projeto SciELO/FapUnifesp.

Todos os colaboradores do Projeto SciELO/FapUnifesp devem considerar as fontes e informação delas derivadas como bens essenciais para o desenvolvimento e operação do Projeto SciELO/FapUnifesp.

Privacidade da Informação sob custódia do Projeto SciELO/FapUnifesp

A privacidade das fontes e informação delas derivada sob custódia do Projeto SciELO/FapUnifesp, armazenadas ou operadas nos meios que o Projeto SciELO/FapUnifesp detém total controle administrativo, físico, lógico e legal, é assegurada por meio das seguintes diretivas:

1. são coletadas de forma ética e legal, para propósitos específicos e devidamente informados;
2. são recebidas pelo SciELO/FapUnifesp, tratadas e armazenadas de forma segura e íntegra;
3. são acessadas somente por pessoas autorizadas e capacitadas para seu uso adequado;
4. podem ser disponibilizadas a empresas contratadas para prestação de serviços, sendo exigido de tais organizações o cumprimento de nossa política e diretivas de segurança e privacidade de dados;
5. é fornecida a terceiros somente mediante autorização prévia ou para o atendimento de exigência legal ou regulamentar;
6. são fornecidas somente aos próprios interessados e mediante solicitação formal, seguindo os requisitos legais vigentes os cadastros, bem como outras solicitações que venham garantir direitos legais ou contratuais.

Criação de Acessos e Conta de E-Mail para Não Colaboradores

A criação de acessos ou contas de e-mail é restrita aos colaboradores, exceto estagiários e jovens aprendizes, mediante solicitação do coordenador responsável e aprovação da Unidade Infraestrutura.

As listas de distribuição e/ou pastas públicas do SciELO/FapUnifesp que possam conter informação destinada à colaboradores não podem ter a participação de terceiros.

Gestão de Acessos

Todos os tipos de sistemas que necessitam de acesso a fontes de informação do Projeto SciELO/FapUnifesp deverão ser rastreados por meio de um controle formal desde a liberação de acesso até a revogação do acesso conforme a Norma de Controle de Acessos na seção

"Gerenciamento de Identidade".

Prevenção de Ataques

TESTE DE INVASÃO

1. Testes de vulnerabilidade devem ser realizados periodicamente, ou quando houver mudança no ambiente, em equipamentos de rede ou aplicações críticas a fim de detectar possíveis falhas;
2. Softwares desenvolvidos, principalmente os que operam na Web, deverão contemplar em seu projeto tanto testes de vulnerabilidade quanto de autenticação, controle de sessão e injeção de código conforme a Norma de Desenvolvimento Seguro.

REGISTRO E MONITORAMENTO DE LOGS

A PSI considera os logs de transações como ferramentas úteis para auditoria de riscos, incidentes, invasões ou para detecção de desvios em privilégios de acesso. Nesse sentido, as seguintes diretrizes são aplicadas:

1. As aplicações e processos devem gerar logs que permitam o monitoramento das atividades realizadas;
2. Os logs devem possuir a operação realizada, data e hora e IP de acesso;
3. Auditoria dos logs deve ser realizada periodicamente a fim de verificar acessos indevidos de usuários;
4. Os registros de log de uso das fontes de informação científicas do Projeto SciELO/FapUnifesp devem ser mantidos indefinidamente;
5. Os registros de log de uso das fontes administrativas devem ser mantidos por no mínimo 12 meses, devendo ser definido em conjunto com o responsável do recurso o prazo a ser mantido. Aplicações de clientes, gerenciados pelo Projeto SciELO/FapUnifesp, devem armazenar informação crítica por no mínimo 5 anos de log;
6. Os logs devem ser mantidos por meios seguros.

PATCHES

Os recursos, aplicativos corporativos devem possuir um procedimento formal de atualização de patches de segurança, sendo que:

1. Deve ser definida a forma de identificação dos patches divulgados pelos fabricantes;
2. O prazo para atualização dos patches;
3. Procedimento para atualização dos patches.

SINCRONIZAÇÃO DE RELÓGIOS

Aplicativos, servidores, acesso físico e recursos deverão ter seu relógio sincronizado para que seja possível realizar a análise criteriosa de incidentes ou de operações de usuários.

NAVEGAÇÃO NA INTERNET

Considera-se a internet meio essencial para busca de informação e produtividade do trabalho, portanto, o uso da mesma, em estações de trabalho está liberado sob monitoramento. Sendo que o monitoramento deve ser capaz de:

1. Detectar os acessos que estão sendo realizados;
2. Detectar as fontes de informação baixadas e enviadas por meio da internet;
3. Identificar possíveis desvios de conduta ou vazamento de informação.

Acesso a sites deverá passar por filtro de conteúdo. Torrent, Pornografia e jogos online são bloqueados.

O manual do colaborador deve conter regras de boa conduta e ética quanto ao uso da internet.

Acesso à Internet em servidores deverá ser bloqueado

REDES E SEGREGAÇÃO DE REDES

Grupos de serviços de informação, usuários e sistemas de informação devem ser segregados em redes.

1. Toda conexão de rede, entrada ou saída deve passar pelo Firewall;
2. As regras do Firewall devem ser analisadas periodicamente a fim de verificar mudanças.
3. O acesso à rede Wireless para visitantes deve estar em uma rede separada da rede corporativa. O acesso dos colaboradores a rede WiFi deve seguir os mesmos critérios de segurança do acesso à rede por fio.

CONEXÃO A REDE DE TERCEIROS

A conexão à rede de terceiros deverá ser analisada previamente quanto a sua segurança e necessidade. E quando necessário deverá seguir todos os critérios de segurança, assim como testes de vulnerabilidade, a fim de mitigar riscos quanto à segurança da informação e continuidade do negócio.

ESTAÇÕES E SERVIDORES

1. Estação de trabalho e servidores deverão ter controle de sessão inativa. Deverá ser feito o bloqueio automaticamente após um período de inatividade, sendo no máximo 3 minuto para servidores e 5 minutos para colaboradores;
2. Estações de trabalho e servidores deverão possuir antivírus instalados e atualizados, e não podem ser desabilitados por usuários comuns;
3. Estações de trabalho deverão possuir acesso através de um controlador de domínio ou um centralizador de autenticação;
4. Não é permitido o compartilhamento de pastas nos computadores de colaboradores do Projeto SciELO/FapUnifesp. Os dados que necessitam de compartilhamento devem ser alocados nos servidores apropriados, atentando às permissões de acesso aplicáveis aos

referidos dados

MÍDIAS REMOVÍVEIS

1. Mídias removíveis deverão ser gerenciadas quanto ao uso e sua liberação;
2. Fontes de informação confidenciais somente poderão ser armazenadas em mídias removíveis quando esta for criptografada.

DESENVOLVIMENTO DE SOFTWARE

1. Para o desenvolvimento seguir a Norma de Desenvolvimento Seguro.

HARDENING

Deve existir um padrão de blindagem dos equipamentos hardening para proteção dos recursos. A TI deverá criar os procedimentos para hardening de estação de trabalho, servidores e equipamentos onde possa ser aplicado.

INTERCÂMBIO DE INFORMAÇÃO COM CLIENTES E FORNECEDORES

O intercâmbio de informação com clientes ou fornecedores deve ser realizado por canais seguros.

1. Adotar sempre a prática da criptografia nos meios de comunicação (E-mail, SFTP, gerenciadores de arquivos);
2. Informação confidencial deve ser transferida somente por meios seguros.

GESTÃO DOS BACKUPS

Para garantia da integridade dos sistemas e dados, a área de Infraestrutura é responsável pela realização de cópias de segurança (Backup), conforme a Norma de Backup e Restauração que garante:

1. As aplicações e informação lógicas devem possuir backup de dados realizados de forma periódica
2. Deve ser considerada a utilização de ambientes standby para aplicações críticas;
3. Os backups devem ser armazenados em locais físicos diferentes do ambiente de produção.

Utilização de Pen drives e armazenamento em nuvem

É proibida a utilização de pen drives e/ou acesso. Caso a utilização seja estritamente necessária para atividades, o colaborador deverá justificar ao gestor responsável, que avaliará a possibilidade de liberação seguindo as premissas e necessidades previstas nesta Política.

A utilização de armazenamento em nuvem é permitido apenas no serviço contratado pelo Projeto SciELO/FapUnifesp.

Propriedade Intelectual

O Projeto SciELO/FapUnifesp detém a propriedade intelectual de todos os projetos, criações ou procedimentos desenvolvidos por qualquer colaborador durante o curso de seu vínculo empregatício.

Uso do correio eletrônico (e-mail)

O correio eletrônico fornecido pela Projeto SciELO/FapUnifesp é um instrumento de comunicação interna e externa de conteúdo profissional relativa às atividades exercidas pelos colaboradores. As mensagens não devem comprometer a imagem do Projeto SciELO/FapUnifesp, não podem ser contrárias à legislação vigente e nem aos princípios éticos.

O uso do correio eletrônico é pessoal e o usuário é responsável por toda mensagem

enviada pelo seu endereço. É terminantemente proibido o envio de mensagens que:

1. Contenham declarações difamatórias e linguagem ofensiva;
2. Possam trazer prejuízos a outras pessoas;
3. Sejam hostis e inúteis;
4. Sejam relativas a “correntes”, de conteúdos pornográficos ou equivalentes;
5. Possam prejudicar a imagem da organização;
6. Possam prejudicar a imagem de outras empresas;
7. Sejam incoerentes com as políticas do Projeto SciELO/FapUnifesp.
8. O serviço de e-mail deve observar:
    1. E-mails deverão ser trafegados por canal seguro;
    2. A ferramenta de e-mail deverá ter recurso habilitado e controlado de AntiSpam e controle de conteúdo.

Mensageria Instantânea

A utilização de mensageria instantânea é permitida apenas no serviço contratado pelo Projeto SciELO/FapUnifesp.

Softwares ilegais

O Projeto SciELO/FapUnifesp respeita os direitos autorais dos programas, ou seja, não permite o uso de programas não licenciados. Assim, é terminantemente proibido o uso de programas ilegais (sem licenciamento) e os usuários não têm permissão para instalações, sendo necessário acessar o sistema de suporte da Unidade Infraestrutura para solicitar qualquer tipo de instalação.

Periodicamente, a Unidade Infraestrutura fará auditoria nos dados dos servidores e/ou nos computadores dos usuários, visando garantir a correta aplicação desta norma. Caso sejam encontrados programas não autorizados, estes deverão ser removidos dos computadores. Aqueles que instalarem em seus computadores de trabalho tais programas não autorizados, se responsabilizam perante o Projeto SciELO/FapUnifesp por quaisquer problemas ou prejuízos causados oriundos desta ação.

Inventário de Ativos

Recursos devem ser monitorados quanto a sua capacidade e atender o crescimento do Projeto SciELO/FapUnifesp. Deve ter um procedimento com pontos críticos a serem monitorados, por exemplo, espaço para armazenamento do log, espaço para crescimento do banco de dados, espaço para recuperação e testes de banco de dados ou aplicativos, capacidade de rede, energia, internet para acesso dos usuários ou colaboradores.

1. Todos os softwares e recursos da empresa devem ser inventariados e controlados pela Unidade Infraestrutura;
2. Não é permitida a instalação de nenhum software sem o consentimento da Unidade Infraestrutura;
3. Não é permitido contratar e utilizar nenhum software para uso organizacional, nas nuvens, sem o consentimento da Unidade Infraestrutura;
4. Não é permitido comprar ou instalar algum equipamento ou recurso sem o consentimento da Unidade Infraestrutura;
5. A Unidade Infraestrutura deverá ter processos para detecção de softwares instalados;
6. Ativos em posse de colaboradores e fornecedores deve ser controlado, em caso de desligamento ou encerramento de contrato o ativo deverá ser devolvido conforme procedimento estabelecido pela Unidade Infraestrutura;
7. Software devem possuir gestão de suas licenças e uso controlado pela Unidade Infraestrutura.
8. Não é permitido a instalação de software não licenciado.

Descarte, destruição e reutilização de equipamentos e mídias

Todas as mídias utilizadas na operação dos processos do SGSI devem ser guardadas, reutilizadas e destruídas de forma segura e protegida, conforme Norma de Classificação e Manuseio da Informação, seção "Sanitização de Mídias".

Mesa e Tela Limpas

Todos os profissionais colaboradores e prestadores de serviços são responsáveis pelas fontes de informação armazenados em seus postos de trabalho (mesa e computador) e devem garantir a segurança das mesmas sendo consideradas boas práticas:

1. Os equipamentos devem ser utilizados com cuidado visando garantir sua preservação e seu funcionamento adequado;
2. Computadores de mesa (desktops) ou dispositivos móveis (notebooks; tablets) devem ser desligados no final do expediente ou sempre que um usuário estiver ausente por um período prolongado;
3. O bloqueio de tela deve ser protegido por senha e deverá ser ativado sempre que o usuário se afastar do computador de mesa ou móvel que esteja utilizando, e realizar (logoff) quando não for mais fazer uso, ou se ausentar por um longo período;
4. Devem ser retirados da mesa de trabalho: papéis, anotações e lembretes que contenham informação ou dados relativos a clientes, senhas e informação interna e restrita. Deve adotar sistema de gerenciamento de senhas;
5. Armazenar informação confidencial em local apropriado;
6. Deixar todos os documentos e dispositivos eletrônicos, no final do dia de trabalho devidamente guardados/organizados.

Papéis e Responsabilidades

É dever de todos – colaboradores, estagiários, aprendizes e prestadores de serviços do Projeto SciELO/FapUnifesp – cumprir com as seguintes obrigações:

Colaboradores, estagiários, aprendizes e prestadores de serviços

Define-se como necessária a classificação de toda a informação de propriedade do Projeto SciELO/FapUnifesp ou sob sua custódia, de maneira proporcional ao seu valor, para possibilitar o controle adequado da mesma:

1. Zelar continuamente pela proteção das fontes de informação do Projeto SciELO/FapUnifesp contra acesso, modificação, destruição ou divulgação não autorizada;
2. Assegurar que os recursos (computacionais ou não) colocados à sua disposição sejam utilizados apenas para as finalidades estatutárias do Projeto SciELO/FapUnifesp;
3. Garantir que os sistemas e fontes de informação sob sua responsabilidade estejam adequadamente protegidos;

4. Garantir a continuidade do processamento da informação crítica para os negócios do Projeto SciELO/FapUnifesp;
5. Cumprir as leis e normas que regulamentam os aspectos de propriedade intelectual e licenças CC-BY;
6. Atender às leis e regras que regulamentam as atividades do projeto;
7. Selecionar de maneira coerente os mecanismos de segurança da informação, balanceando fatores de risco, tecnologia e custo;
8. Comunicar imediatamente à Unidade Infraestrutura qualquer descumprimento da PSI e/ou dos procedimentos de Segurança da Informação;
9. Manter total sigilo sobre informação obtida em decorrência da relação empregatícia, sendo vedada qualquer forma de transmissão e uso de tal informação em relação a terceiros ou para uso pessoal;

Gestor de segurança da informação (GSI.)

O Gestor de Segurança da Informação (GSI) corresponde a um representante indicado e aprovado pela Direção do Programa SciELO (Direção), com o intuito de definir e apoiar estratégias necessárias à implantação e manutenção do SGSI.

Compete ao GSI.:

1. Propor ajustes, aprimoramentos e modificações na estrutura normativa do SGSI., submetendo à aprovação da Direção;
2. Redigir o texto das normas e procedimentos de segurança da informação, submetendo à aprovação da Direção;
3. Requisitar informação das demais áreas do Projeto SciELO/FapUnifesp, por meio das diretorias, gerências, com o intuito de verificar o cumprimento da política, das normas e procedimentos de segurança da informação;
4. Receber, documentar e analisar casos de violação da política e das normas e procedimentos de segurança da informação;
5. Estabelecer mecanismos de registro e controle de eventos e incidentes de segurança da informação, bem como, de não conformidades com a política, as normas ou os procedimentos de segurança da informação;
6. Notificar as gerências e diretorias quanto a casos de violação da política e das normas e procedimentos de segurança da informação;
7. Receber sugestões dos gestores da informação para implantação de normas e procedimentos de segurança da informação;
8. Propor projetos e iniciativas relacionadas à melhoria da segurança da informação;
9. Acompanhar o andamento dos projetos e iniciativas relacionados à segurança da informação;
10. Propor a relação de gestores da informação;
11. Realizar, sistematicamente, a gestão dos ativos da informação;
12. Gerir a continuidade dos negócios, demandando junto às diversas áreas da empresa, Planos de Continuidade dos Negócios, validando-os periodicamente. O Plano de Continuidade de Negócios deve ser definido, implementado e testado a fim de garantir a

disponibilidade dos sistemas de informação;
13. Realizar, sistematicamente, a gestão de riscos relacionados à segurança da informação;
14. Adotar mecanismos automatizados, sempre que possível, para gerenciamento, prevenção e detecção de eventos de segurança;
15. Implementar mecanismos para proteção da segurança física a fim de prevenir danos e acessos não autorizados à informação;
16. Adotar processos de autenticação e controle de acesso seguro para os sistemas de informação;
17. Deliberar sobre o uso de ferramentas de proteção contra softwares maliciosos, vírus, spam, phishing scan e outros dispositivos que possam ameaçar os sistemas de informação da organização.

Coordenadores e Gerentes

Cabe a cada coordenador e ao diretor dominar todas as regras de negócio necessárias à criação, manutenção e atualização de medidas de segurança relacionadas ao ativo de informação sob sua responsabilidade, seja este de propriedade do Projeto SciELO/FapUnifesp ou sob sua custódia.

Os mesmos podem delegar sua autoridade sobre o ativo de informação, porém, continua sendo dele a responsabilidade final pela sua proteção.

Compete a este papel:

1. Classificar, com o apoio do GSI, a informação sob sua responsabilidade, inclusive aquela gerada pelos periódicos, fornecedores ou outras entidades externas, que devem participar do processo de definição do nível de sigilo da informação;
2. Utilizar o Sistema de Gestão de Riscos como instrumento gerencial estratégico para assegurar os requisitos de negócio da organização;
3. Inventariar todos os ativos de informação sob sua responsabilidade;
4. Enviar ao GSI, quando solicitado, relatórios sobre a informação e ativos de informação sob sua responsabilidade. Os modelos de relatórios serão definidos pelo GSI. e aprovados pela Diretoria;
5. Sugerir procedimentos ao GSI. para proteger os ativos de informação, conforme a classificação realizada, além da estabelecida pela Política de Segurança da Informação e Privacidade e pelas Normas de Segurança da Informação;
6. Manter um controle efetivo do acesso à informação, estabelecendo, documentando e fiscalizando a política de acesso à mesma. Tal política deve definir quais usuários ou grupos de usuários têm real necessidade de acesso à informação, identificando os perfis de acesso;
7. Reavaliar, periodicamente, as autorizações dos usuários que acessam as informação sob sua responsabilidade, solicitando o cancelamento do acesso dos usuários que não tenham mais necessidade de acessar a informação;
8. Participar da investigação dos incidentes de segurança e privacidade relacionados à informação sob sua responsabilidade;

9. Cumprir e fazer cumprir a política, as normas e procedimentos de segurança da informação e privacidade;
10. Assegurar que suas equipes possuam acesso e entendimento da política, das normas e dos procedimentos de Segurança da Informação e privacidade;
11. Sugerir ao GSI, de maneira proativa, procedimentos de segurança da informação e privacidade relacionados às suas áreas;
12. Redigir e detalhar, técnica e operacionalmente, as normas e procedimentos de segurança da informação e privacidade relacionados às suas áreas, quando solicitado pelo GSI;
13. Comunicar imediatamente ao GSI. eventuais casos de violação da política, de normas ou de procedimentos de segurança da informação e privacidade.

Diretoria

A Diretoria do SciELO/FapUnifesp está comprometida com o sistema de gestão de segurança da informação e privacidade devendo:

1. Estabelecer as responsabilidades e atribuições pertinente à Gestão da Segurança da Informação;
2. Assegurar que a política e os objetivos de segurança da informação sejam estabelecidos, de forma compatível com a orientação estratégica do Projeto SciELO/FapUnifesp;
3. Promover a integração dos requisitos do sistema de gestão de segurança da informação aos processos do Projeto SciELO/FapUnifesp;
4. Prover os recursos necessários para o sistema de gestão de segurança da informação estão disponíveis;
5. Comunicar a importância da gestão eficaz da segurança da informação, e do cumprimento dos requisitos do sistema de gestão da segurança da informação e privacidade;
6. Certificar que o sistema de gestão de segurança da informação alcança seus resultados pretendidos;
7. Coordenar e incentivar as pessoas a contribuir com a eficácia do sistema de gestão da segurança da informação e privacidade;
8. Promover a melhoria contínua do SGSI e;
9. Apoiar outras funções relevantes de gerenciamento quando demonstrem sua liderança e como ela se aplica às suas áreas de responsabilidade.
10. Aprovar a política e as normas de segurança da informação e suas revisões;
11. Aprovar quem assumirá o papel de GSI;
12. Receber, por intermédio do GSI, relatórios de violações da política e das normas de segurança da informação, quando aplicável;
13. Tomar decisões referentes aos casos de descumprimento da política e das normas de segurança da informação, mediante a apresentação de propostas do GSI;

Consultoria Jurídica

Cabe, adicionalmente, à Consultoria Jurídica, intermediada pelo setor de Administração.

1. Manter o GSI. informado sobre eventuais alterações legais e/ou regulatórias que impliquem responsabilidade e ações envolvendo a gestão de segurança da informação;
2. Incluir na análise e elaboração de contratos, sempre que necessárias cláusulas específicas relacionadas à segurança da informação;
3. Avaliar, quando solicitado, a política, as normas e os procedimentos de segurança da informação.

Área Administrativa

Cabe, adicionalmente, à Área Administrativa:

1. Assegurar-se de que os colaboradores, estagiários, aprendizes e prestadores de serviços comprovem, por escrito, estar cientes da estrutura normativa do GSI. e dos documentos que a compõem;
2. Para os novos colaboradores, prestadores de serviços e estagiários deve ser aplicado o treinamento em segurança da informação em até 15 dias após o início de suas atividades, sendo de responsabilidade de seu gestor a supervisão durante este período;
3. Ter planos de reciclagem das normas internas do SciELO/FapUnifesp;
4. Criar mecanismos para informar, antecipadamente aos fatos, ao canal de atendimento técnico mais adequado, alterações no quadro funcional do SciELO/FapUnifesp.

Área de Qualidade

Coordenada pela área de Infraestrutura. Cabe à área de Qualidade:

1. Consolidar e coordenar a implantação, execução, monitoramento e melhoria do SGSI.;
2. Prover a informação de gestão de segurança da informação;
3. Coordenar as reuniões de análise crítica do SGSI bem como acompanhar os planos de ação resultantes deste fórum;
4. Facilitar a conscientização, a divulgação e o treinamento quanto à política, às normas e os procedimentos de segurança da informação;
5. Efetuar auditorias e inspeções de conformidades periódicas, bem como avaliar a eficácia, acompanhar o atendimento dos respectivos planos de ação e promover a melhoria contínua;
6. Desenvolver um programa de treinamento para os colaboradores e contratados de forma a conscientizar sobre as responsabilidades de cada um em relação à segurança da informação;
7. Gerenciar mudanças organizacionais a fim de garantir os aspectos de disponibilidade, integridade e confidencialidade da informação;
8. Informar todos os colaboradores e contratados sobre a importância da Segurança da Informação, e a necessidade de seguir a Política, Normas, Procedimentos e Instruções referentes ao Sistema de Gestão de Segurança da Informação (SGSI);
9. Estabelecer normas e procedimentos referentes à obrigatoriedade de divulgação dos eventos e incidentes de segurança por todos os colaboradores, bem como as respectivas

penalidades pelo não cumprimento deste objetivo;
10. Executar projetos e iniciativas visando aprimorar a segurança da informação no SciELO/FapUnifesp.

Desenvolvimento

- Profissionais do ciclo produtivo de software (Desenvolvedores, analistas, testadores, suporte) deverão ser treinados quanto às boas práticas de segurança da informação no desenvolvimento de software;
- Boas práticas utilizadas no desenvolvimento seguro de software deverão ser comunicadas a toda a equipe.

Infraestrutura

O setor de infraestrutura de TI é responsável por garantir a disponibilidade, confiabilidade e desempenho dos recursos tecnológicos e de rede necessários para suportar as operações do SciELO/FapUnifesp. As principais responsabilidades do setor de infraestrutura de TI incluem:

- Planejamento e projeto de infraestrutura: O setor de infraestrutura é responsável por planejar, projetar e implementar a infraestrutura tecnológica necessária para atender às necessidades atuais e futuras do SciELO/FapUnifesp. Isso pode incluir servidores, redes, sistemas de armazenamento, bancos de dados, serviços de nuvem, entre outros.
- Configuração e manutenção de hardware e software: Isso envolve a instalação, configuração e manutenção de hardware e software de TI, como servidores, roteadores, switches, firewalls, sistemas operacionais, aplicativos, antivírus e outras ferramentas de segurança.
- Monitoramento e suporte: O setor de infraestrutura de TI é responsável por monitorar a disponibilidade, desempenho e segurança dos sistemas e recursos de TI, identificando e resolvendo proativamente problemas e incidentes para minimizar o tempo de inatividade e garantir a continuidade dos serviços de TI.
- Gestão de rede: Isso inclui a configuração, monitoramento e manutenção de redes de comunicação, como LANs (Redes Locais) e WANs (Redes de Área Ampla), switches, roteadores, acesso à Internet, VPNs (Redes Virtuais Privadas) e outros componentes de rede.
- Gerenciamento de armazenamento e backup: O setor de infraestrutura de TI é responsável pelo gerenciamento de armazenamento de dados, incluindo o planejamento, configuração e monitoramento de sistemas de armazenamento, como SANs (Storage Area Networks), NAS (Network-Attached Storage) e backup de dados para garantir a integridade e disponibilidade dos dados.
- Segurança da informação: O setor de infraestrutura de TI é responsável por implementar e manter políticas e práticas de segurança da informação para proteger os recursos de TI da organização contra ameaças internas e externas. Isso pode incluir a implementação de firewalls, sistemas de detecção e prevenção de intrusões, gerenciamento de identidade e acesso, entre outros controles de segurança.

- Gestão de fornecedores: O setor de infraestrutura de TI pode ser responsável por gerenciar relacionamentos e contratos com fornecedores de hardware, software, serviços de nuvem e outros provedores de serviços de TI, incluindo a avaliação de propostas, negociação de contratos e acompanhamento do desempenho dos fornecedores.
- Planejamento de capacidade: O setor de infraestrutura de TI é responsável por monitorar o uso atual e previsto dos recursos de TI e planejar a capacidade adequada para garantir o desempenho e disponibilidade dos sistemas e serviços de TI.
- Continuidade de negócios e recuperação de desastres: Isso envolve o planejamento, implementação e teste de planos de continuidade de negócios e recuperação de desastres para garantir a resiliência dos sistemas de TI em caso de interrupções, como desastres naturais, falhas de hardware, ataques cibernéticos ou outros eventos adversos. Isso pode incluir a implementação de medidas de backup e recuperação, planos de contingência, procedimentos de resposta a incidentes e testes regulares para garantir a eficácia dos planos de continuidade de negócios.
- Atualização e patches: O setor de infraestrutura de TI é responsável por garantir que os sistemas operacionais, aplicativos e outros componentes de infraestrutura de TI sejam atualizados regularmente com os patches de segurança mais recentes e atualizações de software. Isso é importante para garantir que os sistemas sejam protegidos contra vulnerabilidades conhecidas e para manter a estabilidade e desempenho dos sistemas.
- Gerenciamento de ativos de TI: Isso envolve o rastreamento e gerenciamento de ativos de hardware e software da organização, incluindo servidores, roteadores, switches, licenças de software, entre outros. O setor de infraestrutura de TI é responsável por manter registros precisos de ativos de TI, gerenciar sua alocação, uso, manutenção e descarte adequado.
- Documentação e padrões: O setor de infraestrutura de TI é responsável por criar e manter documentação técnica, incluindo manuais, procedimentos operacionais padrão, diagramas de rede, políticas de segurança e outros documentos relacionados à infraestrutura de TI. Além disso, o setor de infraestrutura de TI é responsável por estabelecer e fazer cumprir padrões e diretrizes de configuração, desempenho, segurança e melhores práticas em toda a infraestrutura de TI.
- Suporte técnico: O setor de infraestrutura de TI fornece suporte técnico aos usuários finais e a outros departamentos do SciELO/FapUnifesp para resolver problemas técnicos relacionados à infraestrutura de TI, como conectividade de rede, problemas de hardware, configuração de software e outras questões técnicas.

MELHORIA CONTÍNUA

- Treinamentos focados em segurança da informação deverão ocorrer com frequência, a fim de conscientizar a importância para os colaboradores e aprimorar os controles existentes;
- Deve ser considerado a contratação ou benchmark com outras empresas considerando a melhoria do processo de segurança da informação e privacidade.

Auditoria Interna

Todo ativo de informação sob responsabilidade do SciELO/FapUnifesp é passível de auditoria em data e horários determinados pelo GSI. Contudo, se observadas práticas que não respeitam as diretrizes desta Política, podem ser realizados registros dos problemas encontrados e ações corretivas serão exigidas.

A realização de uma auditoria deverá ser obrigatoriamente aprovada pela Diretoria e, durante a sua execução, deverão ser resguardados os direitos quanto à privacidade de informação pessoal, desde que estas não esteja disposta em ambiente físico ou lógico de propriedade do SciELO/FapUnifesp de forma que se misture ou impeça o acesso à informação de propriedade ou sob sua responsabilidade.

Com o objetivo de detectar atividades anômalas de processamento da informação e violações da política, das normas ou dos procedimentos de segurança da informação, a área de TI poderá realizar monitoramento e controle proativos, mantendo a confidencialidade do processo e da informação obtidas.

Em ambos os casos, a informação obtida poderá servir como indício ou evidência em processo administrativo e/ou legal.

As auditorias internas são planejadas com foco na análise do atendimento de todos os processos relacionados ao SGSI e nos resultados de auditorias anteriores.

As auditorias internas devem ser realizadas uma vez ao ano, por auditores internos ou externos, capacitados e treinados, com conhecimento nas normas ISO 27001 e LGPD e conhecimento dos processos do SciELO/FapUnifesp. Deve haver independência, garantindo que auditores não auditem os processos em que estejam envolvidos.

As auditorias externas devem ser realizadas para manter a validade das certificações definidas.

Ação Corretiva

Quando identificadas não conformidades na execução dos processos ou durante as auditorias internas ou externas, estas devem ser registradas para análise e tratamento.

Toda a não conformidade registrada deve ter a causa identificada. Devem ser tomadas ações para eliminação dessas causas e verificada a eficácia das ações.

Contato com Autoridades

A gestão dos contatos com autoridades é da responsabilidade da Gerência de Segurança da Informação e/ou da Gerência Administrativa que deve:

1. Consolidar, comunicar e divulgar em repositório conhecido e acessível do SciELO/FapUnifesp a lista dos contatos atualizados periodicamente;
2. Realizar testes periódicos e amostrais dos contatos registrados com o intuito de avaliar que são adequados e eficazes

Nota* A lista deve possuir data de emissão da última versão, nome do responsável pelas atualizações, classificação da informação.

O Acionador é a pessoa qualificada para avaliar se deve proceder com o acionamento. É o ponto focal que deve ser conhecido por todos na organização para avaliar os eventos identificados e proceder com o adequado acionamento.

Cabe ao Acionador manter contato regular com as autoridades com o assegurar a eficácia no acionamento numa situação de crise.

Cada acionador deve possuir um par designado para atuar na ausência deste. Este contato deve figurar como alternativa na tabela de contato com autoridades.

CONTATO COM AUTORIDADES		
ENTIDADE / ÓRGÃO	**TIPO DE OCORRÊNCIA**	**ACIONADOR**
Bombeiro / Defesa Civil	Emergência: Incêndios, terremotos, enchentes, catástrofes, etc.	Gerência Administrativa
Fornecedores de água / eletricidade	Interrupção ou desabastecimento do fornecimento de energia, água, etc.	Gerência Administrativa
Provedores de links / Internet	Para relatar incidentes de ataques de vírus e de hackers sofridos.	Gerente de Infraestrutura
	Interrupção / lentidão do Serviço.	Gerente de Infraestrutura
Polícia Militar / Polícia Civil	Situações de conflito, agressões, crimes, sequestro, ações terroristas e assemelhados.	Gerência Administrativa
Certificadora ISO	Alterações de escopo de certificação, modificações na infraestrutura, sistemas, pessoas, produtos e serviços que tenham impacto considerável no SGSI.	Gerente de Infraestrutura
Autoridade Certificadora	Revogação / Renovação de certificados digitais.	Gerente de Infraestrutura
Polícia Federal	Crimes informáticos, fraudes eletrônicas e assemelhados	Gerência Administrativa
ANPD	Autoridade nacional de Proteção de Dados – incidentes, registros e RIPD relativos ao tratamento de Dados Pessoais	Gerente de Infraestrutura

Contato com Grupos Especialistas

A Gerência de Infraestrutura deve manter efetivo contato e participação com grupos de especialistas reconhecidos.

Análise Crítica do SGSI

A organização deve realizar a análise crítica do SGSI minimamente uma vez ao ano. Esta análise deve ter a participação direta da Diretoria e deve considerar:

1. O resultado das ações de análises críticas anteriores do SGSI;
2. Mudanças em questões externas e internas que são relevantes para o sistema de gestão da segurança da informação;
3. Retroalimentação sobre o desempenho da segurança de informação, incluindo as tendências de:
    1. Não-conformidades e ações corretivas;
    2. Resultados de monitoramento e medição;
    3. Resultados de auditoria internas ou externas do SGSI e;
    4. Cumprimento dos objetivos da segurança da informação.

4. Comentários das partes interessadas;
5. Os resultados da avaliação de risco e a situação do plano de tratamento do risco;
6. Oportunidades para a melhoria contínua;
7. Impactos de mudanças ocorridas ou que possam ocorrer (mudanças organizacionais, mudanças em procedimentos de tratamento de dados pessoais, mudanças decorrentes de decisões governamentais, entre outros).

As saídas das análises críticas devem incluir decisões relacionadas com oportunidades de melhoria contínua e qualquer necessidade de mudança no sistema de gestão da segurança da informação.

O SciELO/FapUnifesp deve manter informação documentada como evidência dos resultados das análises críticas pela Diretoria

Denúncias

Qualquer descumprimento desta Política, ou ainda suspeitas ou evidências devem ser reportadas a ouvidoria SciELO/FapUnifesp através do e-mail ouvidoria@scielo.org.

Violações e Sanções

Violações

São consideradas violações à política, às normas ou aos procedimentos de segurança da informação as seguintes situações, não se limitando às mesmas:

1. Quaisquer ações ou situações que possam expor o SciELO/FapUnifesp à perda financeira e de imagem, direta ou indiretamente, potenciais ou reais, comprometendo seus ativos de informação;
2. Utilização indevida de dados corporativos, divulgação não autorizada de informação, segredos comerciais ou outra informação sem a permissão expressa do Gerente ou Diretoria;
3. Uso de dados, informação, equipamentos, software, sistemas ou outros recursos tecnológicos, para propósitos ilícitos, que possam incluir a violação de leis, de regulamentos internos e externos, da ética ou de exigências de organismos reguladores da área de atuação do SciELO/FapUnifesp ou de seus clientes;
4. Descumprir alguns dos itens estabelecidos nesta política de segurança;
5. A não comunicação imediata à área de Ouvidoria de quaisquer descumprimentos da política, de normas ou de procedimentos de Segurança da Informação, que porventura um colaborador, estagiário, aprendiz ou prestador de serviços venha a tomar conhecimento ou chegue a presenciar.

Sanções

A violação à política, às normas ou aos procedimentos de segurança da informação ou a não aderência à PSI do Projeto SciELO/FapUnifesp são consideradas faltas graves, podendo ser aplicadas as seguintes sanções: advertência formal, suspensão, rescisão do contrato de trabalho outra ação disciplinar e/ou processo civil ou criminal. Podem ainda ocorrer sanções definidas pelo GSI sempre respeitando a legislação vigente.

Também serão observadas e aplicadas as penalidades previstas na Consolidação das Leis de Trabalho – CLT.

Revisão e Manutenção

Esta norma deverá ser revisada anualmente ou quando uma mudança significativa ocorrer na organização.

Histórico de Revisões

Versão	Data	Descrição	Autor

1.0	01/04/2021	Elaboração do documento	Rondineli Saad
1.0	05/04/2022	Revisão do documento	Rondineli Saad
1.0	08/11/2022	Revisão do documento	Abel Packer
1.0	21/11/2022	Aprovação do documento	Abel Packer
1.1	18/04/2023	Revisão do Documento	Rondineli Saad

Aprovação do Documento

Nome	Cargo	Assinatura	Data
Abel Packer	Diretor		10/11/2022
Luís Gomes	Coordenador Unidade Administração		10/11/2022
Rondineli Saad	Gestor de Segurança da Informação		10/11/2022