MANTENEDORA

FUNVIC – FUNDAÇÃO UNIVERSITÁRIA VIDA CRISTÃ

MANTIDO

UNIFUNVIC

CENTRO UNIVERSITÁRIO FUNVIC

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DO UNIFUNVIC

PINDAMONHANGABA/SP

2024

CENTRO UNIVERSITÁRIO FUNVIC – UNIFUNVIC

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

A Política de Segurança da Informação (PSI) do UniFUNVIC é um documento que define, orienta e estabelece as diretrizes corporativas institucionais para a proteção dos ativos de informações e a prevenção de responsabilidade legal para todos os usuários.

A PSI possibilitar o gerenciamento da segurança de informação em uma organização, estabelecendo regras e padrões para proteção das informações sensíveis e críticas de uma organização. Ela define um conjunto de ações, procedimentos, diretrizes e práticas para garantir a confidencialidade, integridade e disponibilidade das informações, bem como para minimizar os riscos de perda ou roubo dessas informações.

A PSI é uma ferramenta importante para ajudar a instituição a lidar com ameaças de segurança cibernética cada vez mais sofisticadas e frequentes. Ele identifica os riscos que as informações enfrentam e propõe medidas de segurança para mitigá-los, levando em consideração as melhores práticas de segurança da informação e os requisitos legais e regulatórios aplicáveis.

A política e o seu respectivo plano de ação, deve ser adaptado às necessidades específicas da organização, levando em conta seu tamanho, estrutura, ativos e processos críticos, além dos riscos que ela enfrenta. O objetivo final dessa política é garantir a continuidade das finalidades e dos negócios institucionais, e minimizar as perdas financeiras e reputacionais decorrentes de violações de segurança da informação.

A PSI, requer uma abordagem cuidadosa e estratégica, deve ser elaborado com base em uma análise de riscos, identificando ameaças, vulnerabilidades e impactos potenciais. A partir daí, são definidas as medidas de segurança adequadas para minimizar esses riscos, como políticas de acesso, backup e recuperação de dados, além de controles físicos e lógicos.

Destacamos algumas etapas essenciais para elaborar um plano de ação de segurança da informação eficiente, acompanhe:

Análise de riscos

A análise de risco nas políticas de segurança de uma Instituição de Ensino Superior (IES) é fundamental para proteger dados pessoais, informações sensíveis e garantir a continuidade dos serviços prestados. Dada a alta demanda por serviços digitais e a crescente quantidade de informações acadêmicas e administrativas trafegadas diariamente, a IES está exposta a diversas ameaças, tanto no ambiente cibernético quanto no físico.

Podemos incluir brechas nos sistemas de autenticação, falhas de segurança em servidores de dados, permissões inadequadas em sistemas de gestão acadêmica, e até mesmo o acesso físico a áreas restritas da instituição. Além disso, políticas insuficientes de controle de acesso e a falta de práticas consistentes de atualização de software deixam o ambiente suscetível a ataques como phishing, ransomware e engenharia social.

A avaliação de ameaças deve considerar diferentes vetores de ataque:

- **Ataques cibernéticos**: tentativas de invasão aos sistemas da universidade, visando roubar informações sensíveis, como dados pessoais de alunos e funcionários ou resultados de pesquisas confidenciais.
- **Ameaças internas**: ações indevidas realizadas por colaboradores, intencionais ou não, que podem expor a IES a falhas de segurança.
- **Riscos de compliance**: a falta de adequação às leis de proteção de dados, como a LGPD (Lei Geral de Proteção de Dados), pode resultar em sanções legais e perda de reputação.

Definição de políticas de segurança

As políticas de segurança são as diretrizes que vão guiar o comportamento dos usuários da rede. É importante que elas sejam claras, objetivas e simples para que todos possam entender e seguir.

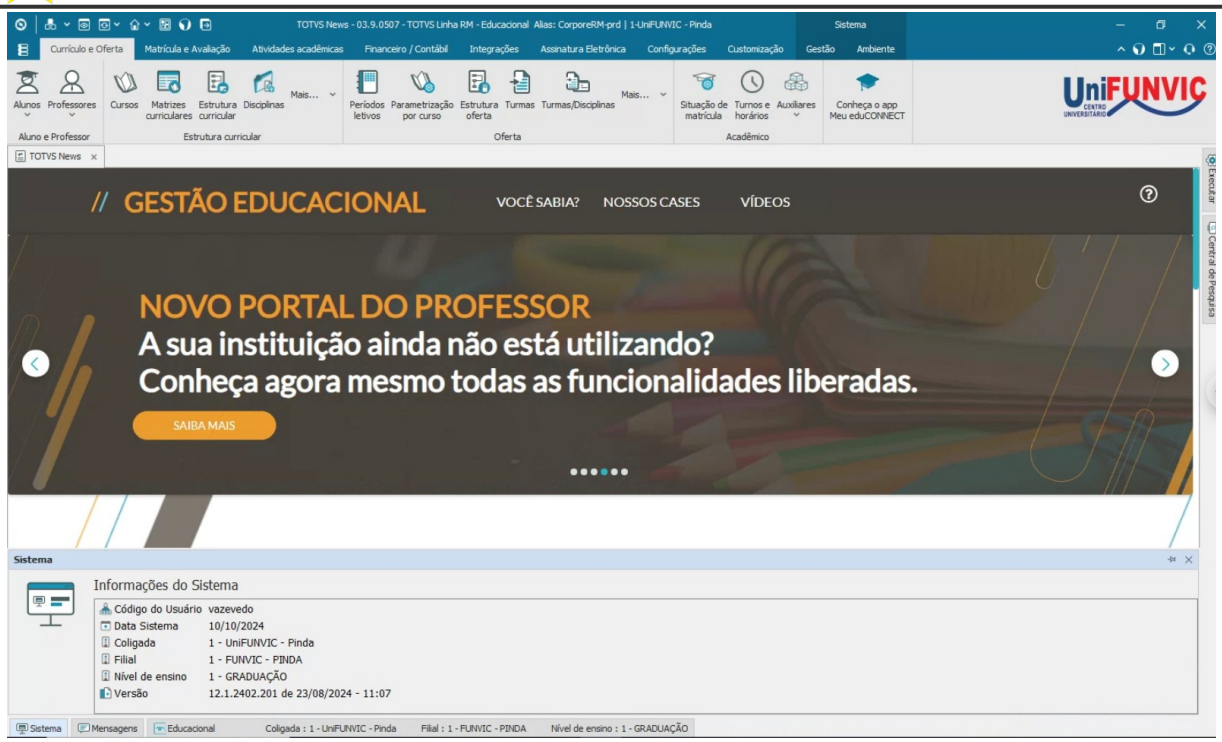
Seleção de controles de segurança

A I.E.S. implementa políticas rigorosas de segurança cibernética, focadas na restrição de acesso a sites indesejados e protocolos de rede potencialmente maliciosos. Essas diretrizes visam proteger a integridade da rede institucional e garantir um ambiente de aprendizado seguro.

Por meio do sistema de gerenciamento, a instituição adota servidores DNS externos que possibilitam o bloqueio de acesso por categorias específicas. Essa abordagem proporciona uma flexibilidade aprimorada e uma camada adicional de segurança, complementando o sistema de firewall existente. Assim, garantimos uma rede mais segura e controlada, alinhada às diretrizes da Universidade para promover um ambiente acadêmico protegido e produtivo.

A I.E.S. utiliza o sistema de gestão educacional TOTVS, uma solução consolidada no mercado que oferece robustez e eficiência na gestão interna. Entre suas diversas ferramentas, o TOTVS visa facilitar a interação entre a instituição e os alunos, proporcionando uma experiência integrada e eficiente.

Destaca-se que o TOTVS implementa medidas de segurança avançadas, incluindo o uso de bancos de dados criptografados, o que reforça a proteção das informações sensíveis. Além disso, o sistema está em conformidade com as políticas de proteção de dados, como a LGPD, assegurando a privacidade e a integridade das informações dos usuários. Dessa forma, o TOTVS se posiciona como uma solução de alta qualidade e segurança para a gestão educacional da I.E.S



Atualmente, o sistema está hospedado na nuvem, utilizando uma arquitetura que inclui servidores dedicados para homologação, produção e teste. Essa estrutura permite uma gestão eficiente por parte da equipe de TI, assegurando a integridade e a funcionalidade do sistema em diferentes ambientes.

A alocação em nuvem proporciona robustez e escalabilidade, além de incorporar medidas de segurança rigorosas, como criptografia de dados em trânsito e em repouso, autenticação multifatorial e monitoramento contínuo. Essas práticas garantem que o sistema permaneça extremamente seguro, protegendo as informações sensíveis e assegurando a conformidade com as normativas de segurança e privacidade.

Reforçando a política de segurança, a I.E.S. implementa o uso de e-mails corporativos e institucionais para alunos e professores, visando aprimorar a segurança e a gestão da informação. Esta prática assegura que todas as comunicações sejam realizadas em um ambiente controlado e protegido, minimizando riscos associados a vazamentos de dados e acessos não autorizados.

O objetivo da instituição é garantir a segurança dos dados e proporcionar um ambiente educacional de qualidade. Ao utilizar e-mails institucionais, a I.E.S. não apenas protege as informações sensíveis, mas também estabelece um canal confiável para interações

acadêmicas, contribuindo assim para uma experiência de aprendizado segura e eficaz para os alunos.

Atualmente, a I.E.S. implementa diversas ferramentas de segurança, dentre as quais se destaca o uso de cookies para acesso ao sistema e ao site. Cookies são pequenos arquivos de texto que são armazenados em dispositivos durante a navegação, contendo informações relacionadas às preferências do usuário. Esses arquivos permitem melhorar a experiência de uso ao armazenar e recuperar dados sobre os hábitos de navegação, sem conter informações pessoais ou sensíveis, como dados bancários.

Os cookies ocupam um espaço de memória mínimo e a maioria das informações é excluída ao final da sessão. Além disso, é necessário aceitar um termo de compromisso ao acessar as plataformas, reforçando o compromisso da I.E.S. com a segurança da informação em sua estrutura. Essa abordagem visa garantir um ambiente digital seguro e eficiente para todos os usuários.

Na I.E.S., utilizamos servidores de domínio para gerenciar de forma eficiente os perfis e os acessos dos usuários. O servidor de domínio centraliza a autenticação e autorização, permitindo um controle rigoroso sobre as permissões e privilégios de cada usuário. Isso facilita a administração de contas e assegura que os acessos sejam concedidos conforme as diretrizes institucionais.

Complementando essa estrutura, implantamos um servidor de arquivos que, em conjunto com políticas de acesso bem definidas, restringe o acesso a informações confidenciais, garantindo a proteção dos dados sensíveis da instituição.

Adicionalmente, o sistema TOTVS proporciona uma gestão detalhada dos usuários e seus níveis de acesso. Essa funcionalidade permite que o administrador do sistema tenha controle sobre alterações e monitoramento de atividades, ajudando na identificação de possíveis fraudes internas. A combinação do servidor de domínio com as robustas políticas de segurança do TOTVS reforça a integridade e a segurança da informação na I.E.S., promovendo um ambiente digital seguro e controlado.

Os dados em nosso sistema são protegidos por técnicas avançadas de criptografia, assegurando um nível elevado de segurança. Utilizamos o banco de dados Oracle, que oferece robustez e alto desempenho, fundamental para o gerenciamento eficiente das informações.
Além disso, seguimos rigorosamente as políticas de segurança da informação, com especial atenção aos dados sensíveis, conforme as diretrizes da LGPD (Lei Geral de Proteção de Dados). Isso inclui práticas de proteção, armazenamento seguro e controle de acesso, garantindo que as informações pessoais sejam tratadas com a máxima confidencialidade e integridade, em conformidade com a legislação vigente. Essa abordagem reforça nosso compromisso com a proteção dos dados dos usuários e a segurança da informação na I.E.S.

Monitoramento contínuo

Na I.E.S, a utilização do Mikrotik é fundamental para otimizar a segurança e o gerenciamento da rede, garantindo um desempenho eficiente e uma proteção robusta contra ameaças externas.

O Mikrotik é um equipamento que transforma plataformas x86 em roteadores, oferecendo funções como Firewall, VPN, Proxy, Hotspots, QoS e Controle de Banda, conforme a licença adquirida. Utilizando o RouterOS, um sistema operacional baseado em Linux, o Mikrotik proporciona segurança de rede com um firewall que controla o tráfego de dados através de regras predefinidas. Além disso, conta com um cache DNS para acelerar as respostas às consultas.

Treinamento dos usuários

O treinamento de usuários é um componente essencial na implementação de políticas de segurança da informação na Universidade. Esse processo visa garantir que todos os colaboradores, especialmente os novos, compreendam as funcionalidades dos sistemas e as práticas de segurança adotadas para minimizar riscos e assegurar a conformidade com a LGPD (Lei Geral de Proteção de Dados).

Estrutura dos Treinamentos

A Universidade oferece **treinamentos específicos** nas áreas de TI e segurança da informação, abordando os seguintes aspectos:

1. **Treinamento Inicial para Novos Colaboradores**:
    - Os novos colaboradores passam por sessões com a equipe de TI e os funcionários do próprio setor de atuação. Esse treinamento abrange:
        - Apresentação das **funcionalidades dos sistemas** utilizados no ambiente de trabalho.
        - Orientação sobre as **políticas de segurança da informação**, incluindo o uso adequado de credenciais, boas práticas para o armazenamento de dados e proteção contra ameaças cibernéticas.
        - **Conformidade com a LGPD**, destacando a importância de proteger dados pessoais e sensíveis dos alunos, funcionários e outros stakeholders da instituição.

2. **Treinamento Contínuo e de Atualização**:
    - Além do treinamento inicial, a Universidade promove **programas contínuos** de capacitação e atualização, especialmente para áreas mais sensíveis, como a gestão de dados acadêmicos, plataformas de ensino a distância (EAD) e sistemas administrativos. Isso garante que os colaboradores estejam sempre alinhados com as melhores práticas e novidades na área de segurança.

3. **Tutoria e Suporte a Plataformas de Ensino (EAD)**:
    - A universidade conta com uma equipe de **tutoria e suporte** para as plataformas de ensino a distância, que auxilia tanto colaboradores quanto alunos no uso correto das ferramentas, garantindo que os procedimentos de segurança sejam seguidos no ambiente virtual de ensino. Isso inclui:
        - Suporte técnico para o uso das plataformas.
        - Orientação sobre o acesso seguro, prevenção contra ameaças como phishing, e manuseio adequado de conteúdos sensíveis.

- Conteúdo do Treinamento
- Os treinamentos fornecidos abordam uma ampla gama de tópicos relevantes para a segurança da informação, incluindo:
- **Gerenciamento de senhas e autenticação multifator**: Práticas recomendadas para a criação de senhas fortes e o uso de autenticação em duas etapas para acesso aos sistemas.
- **Identificação de ameaças cibernéticas**: Capacitação para reconhecer tentativas de phishing, malwares, e-mails suspeitos e outras técnicas comuns de ataque.
- **Proteção de dados**: Procedimentos de armazenamento e transmissão segura de dados, incluindo criptografia e uso de redes seguras.
- **Responsabilidades no uso de sistemas e dados**: Cada colaborador é treinado sobre suas obrigações em relação ao manuseio de informações e à proteção de dados sensíveis.
- **Conformidade com a LGPD**: Explicação dos direitos dos titulares dos dados e dos deveres da instituição e de seus colaboradores no tratamento de dados pessoais.

A implementação de um programa robusto de **treinamento de usuários** é essencial para o sucesso das políticas de segurança da informação da Universidade. Ao capacitar os colaboradores com conhecimentos técnicos e operacionais, a instituição mitiga riscos, garante a conformidade com a legislação vigente, e preserva a integridade e a confidencialidade das informações, assegurando um ambiente acadêmico e administrativo seguro

Período: Ação contínua

Operacionalização:

a) Realizar séries de estudos sobre as áreas do Curso;

b) Divulgar das atividades de extensão e pesquisa desenvolvidas no UniFUNVIC a toda Comunidade Acadêmica;

c) Analisar e propor em conjunto com o NDE ações de ensino que dialoguem com atividades de extensão e da pesquisa nos planos de ensino; e,

d) Incentivar a criação de representações de turma e suas participações no âmbito do Curso, do UniFUNVIC.

e) Promover e incentivar ações interdisciplinares entre os componentes curriculares e em outros cursos do UniFUNVIC;

f) Criar espaços de diálogo para e com a comunidade acadêmica.

g) Estimular a formação crítica do estudante e o engajamento com os espaços de atuação;

h) Promover rodas de conversas para a construção de relações de integração entre os estudantes, docentes, técnicos-administrativos e colaboradores;

i) Promover discussões e espaços de reflexão de documentos normativos como LDB, Diretrizes Curriculares, Documentos Curriculares, entre outros;

j) Incentivar a representação discente junto ao âmbito do Curso, da Comunidade Acadêmica do UniFUNVIC e a Sociedade Local;

k) Propor junto ao NDE a realização de atividades interdisciplinares entre os componentes curriculares;

l) Organizar ações de acompanhamento pedagógico que visem um melhoramento da prática docente e do andamento das disciplinas;

m) Fomentar discussões interdisciplinares entre as disciplinas pedagógicas teóricas e nas disciplinas pedagógicas com as práticas, a partir de Rodas de conversa entre estudantes, docentes e convidados;

n) Realizar reuniões pedagógicas bimestrais com os professores;

o) Reunir dados e planejar juntamente com o NDE ações para melhoria do rendimento dos estudantes, além da oferta necessária de disciplinas;

p) Buscar alternativas junto a Reitoria do UniFUNVIC para sanar lacunas de aprendizagens:

- Realizar as discussões e planejamentos acadêmicos semestrais;

- Incentivar a participação de estudantes em monitorias, iniciação científica, programas de formação, eventos, mobilidade acadêmica e o intercâmbio;

- Conscientizar e incentivar o estudante sobre a preparação, e importância de sua participação na avaliação do ENADE.

q) Fortalecer o diálogo com associações, conselhos e representações de classes do curso;

r) Incentivar a interação dos coordenadores dos cursos a visitar semanalmente as classes/turmas e colher os feedbacks do Curso;

s) Promover semestralmente a Semana de Capacitação e Planejamento Pedagógico, com encaminhamento

dos planos de ensino para aprovação ao Colegiado do Curso;

t) Incentivar e fortalecer as atividades de estágio curriculares e de iniciação as práticas docentes (Programa de Aprimoramento Profissional – UniFUNVIC), também de seu programa de formação PIBID;

u) Buscar e ampliar as parcerias e os convênios com instituições públicas e privadas, empresas, e serviços;

v) Estimular a criação e participação em projetos de pesquisa, assim como, divulgar os grupos de pesquisa, dando suporte as suas ações e um acompanhamento dos projetos;

w) Incentivar e conscientizar sobre a importância na participação dos estudantes nas ações sociais junto à sociedade local, no âmbito da extensão e do voluntariado, tornando-o protagonista na comunidade;

x) Incentivar e conscientizar sobre a importância na participação dos estudantes em eventos culturais promovidos pela Comunidade Acadêmica do UniFUNVIC, dentro da cosmovisão institucional, assim como com a presença de grupos externos, tornando-o ator (a) da comunidade;

y) Conscientizar e incentivar a participação dos estudantes em atividades informativas e de comunicação, junto ao Canal Universitário e ao FUNVICast;

z) Incentivar a participação no processo avaliativo institucional e compartilhar os resultados com os estudantes e docentes do Curso.

Administração e Política

- Gerenciar democraticamente as ações da Coordenação do Curso;

- Elaborar, executar e prestar contas das atividades da Coordenação do Curso;

- Implementar e dar provimento as recomendações do NDE e decisões do Colegiado do Curso;
- Dar celeridade e acompanhar os processos e trabalhos vinculados ao Curso;
- Melhorar a gestão da infraestrutura dos laboratórios e salas de aula, mantendo espaços e equipamentos adequados à realização das práticas da formação da área do Curso;
- Dar transparência as ações da Coordenação e suas representações;
- Estimular e tornar acessível o uso dos canais de comunicação institucionais como: e-mails, Portal, Redes Sociais Institucionais, Área do Aluno, Ouvidoria;
- Consolidar o uso das Plataformas Educacionais Institucionais (AVA) e a Biblioteca Digital do UniFUNVIC;
- Cumprir e fazer cumprir as normativas do UniFUNVIC.

Período: Ação semanal/Mensal

Operacionalização:

a) Realizar um levantamento de todas as ações que ainda não foram despachadas;
b) Organizar e propor os Regimentos Internos do Curso e do NDE;
c) Propor as atualizações das Normas Internas como Estágio, TCC;
d) Sistematizar os atos normativos do Curso;
e) Organizar e divulgar a agenda virtual da Coordenação para transparência das ações;
f) Publicar notícias, atas, decisões no Site do Curso;
g) Despachar processos em até 2 dias após a finalização das atividades no âmbito do Curso;
h) Organizar e manter organizado e atualizado o sistema de patrimônio do Curso;
i) Efetuar estudos para manutenção e compras de equipamentos do Curso;
j) Organizar a listagem de patrimônio do Curso e presente nos espaços utilizados pelo Curso;
k) Organizar a documentação interna e o trabalho administrativo para a Secretaria Acadêmica;
l) Delegar as ações para as Coordenações e Comissões Internas;
m) Promover conversas e reuniões de trabalhos entre as Coordenações internas;
n) Apoiar as ações das Comissões Internas; e,

o) Divulgar os meios de comunicação do UniFUNVIC e as ações institucionais.

Período: Ação semestral

Operacionalização:

a) Realizar levantamento de dados e informações junto ao NDE para ampliação, troca e/ou melhoria do quadro docente;

b) Articular com a Pró-Reitoria Acadêmica, Pró-Reitoria de Pós-Graduação, Pesquisa, Extensão e Inovação e a Reitoria as possibilidades de adequações e melhorias;

c) Incentivar a qualificação e capacitação técnica dos docentes e colaboradores;

d) Conscientizar e incentivar a publicação científica, como parte integrante da atividade do docente;

e) Estimular a formação continuada através da divulgação e apoio de ações de extensão, grupos de pesquisa e pós-graduação.

Período: Ação Contínua

Operacionalização:

a) Promover discussões sobre a capacitação;

b) Divulgar cursos de formação para capacitação virtual;

c) Colaborar com manutenção do Programa de Excelência Pessoal e Institucional (PEPI);

d) Organizar as ações administrativas e pedagógicas para visita do MEC;

e) Promover discussões com a Comunidade Acadêmica sobre a visita do MEC;

f) Receber e acompanhar as ações da visita do MEC;

g) Promover as discussões internas pós a visita do MEC e seu relatório;

h) Traçar com o Colegiado do Curso e NDE, estratégias para solucionar eventuais problemas apontados pelo relatório da visita do MEC, e apresentar a Pró-Reitoria Acadêmica e Reitoria;

i) Zelar pelo ensino e aprendizagem com qualidade, e a sustentabilidade do Curso.

Período: Ação semestral

a) Verificar com a Secretaria Acadêmica o estado da documentação para a visita do MEC;

b) Organizar a documentação faltante para a vista do MEC;

c) Realizar discussões com o NDE, estudantes e outros cursos sobre a visita do MEC;

d) Promover os espaços para discussões internas da visita do MEC;

e) Buscar com o Colegiado do Curso, NDE e a Pró-Reitoria Acadêmica apoio técnico para a visita do MEC;

f) Acompanhar a equipe da visita do MEC durante a semana de avaliação; e

g) Realizar reuniões internas e com a gestão superior para solucionar eventuais problemas apontados pelo relatório.

Em acordo com a Política de Segurança da Informação aprovamos este documento com o Plano de Segurança da Informação do Centro Universitário FUNVIC – UNIFUNVIC, entrando em vigor no dia 03 de janeiro de 2024.

DE-SE CIÊNCIA, PUBLIQUE-SE E CUMPRA-SE.

SEGUE PORTARIA DE APROVAÇÃO