Política de Segurança da Informação

Segurança da Informação

Histórico do Documento

Versão	Alterações	Autor	Aprovador	Data
01	Emissão Inicial	Leandro Rodrigues - SecureByte	Alan Marcon	DD/MM/2024

Sumário

1. Introdução

A UniFECAF reconhece a importância da segurança da informação para seus negócios e está comprometida em proteger as informações confidenciais de seus clientes, Alunos e Corpo Docente bem como garantir a integridade, confidencialidade e disponibilidade de seus sistemas e dados. Esta Política de Segurança da Informação é baseada nos requisitos da norma ISO 27001 e ISO 27701 e estabelece os princípios e diretrizes a serem seguidos por todos os colaboradores da UniFECAF envolvidos em suas atividades.

2. Escopo

Esta política se aplica a todos os sistemas de informação, processos, colaboradores e terceiros envolvidos nos serviços da UniFECAF.

3. Objetivo

A presente política tem como objetivo:

- Garantir a confidencialidade das informações da UniFECAF e de seus clientes, alunos e corpo docente evitando acesso não autorizado, divulgação ou uso indevido;
- Assegurar a integridade dos dados, prevenindo alterações não autorizadas;
- Garantir a disponibilidade contínua dos sistemas e serviços, evitando interrupções não planejadas;
- Cumprir com as leis, regulamentos e requisitos contratuais aplicáveis à segurança da informação e privacidade de dados;
- Promover a conscientização e a cultura de segurança da informação e privacidade de dados entre os colaboradores.

4. Papéis e Responsabilidades

Alta Direção

Deve fornecer o suporte para a implementação e manutenção do Sistema de Gestão de Segurança da Informação (SGSI), estabelecendo os recursos adequados e demonstrando liderança em relação à segurança da informação.

Gestão da Segurança da Informação

Deve coordenar e/ou executar as atividades necessárias para a implementação e manutenção do SGSI, incluindo a definição de políticas, processos, controles e monitoramento contínuo.

Colaboradores

Todos os colaboradores da UniFECAF devem estar cientes de suas responsabilidades em relação à segurança da informação, seguir as políticas e procedimentos estabelecidos, relatar quaisquer incidentes de segurança e participar de treinamentos e atividades de conscientização.

5. Diretrizes

A UniFECAF deve implementar, manter e promover a melhoria contínua de controles de segurança adequados para proteger seus ativos de informação.

5.1 Gestão de Acesso Lógico à Informação

Garantir que o acesso às informações e sistemas seja concedido apenas a usuários autorizados e de acordo com os privilégios necessários.

- Os acessos aos sistemas e informações confidenciais devem ser concedidos apenas a usuários autorizados, por meio de autenticação adequada;
- Devem ser estabelecidas políticas de senha robustas, exigindo senhas fortes, trocas regulares de senha e restrição do compartilhamento de senhas;
- É necessário implementar controle de acesso baseado em funções, atribuindo privilégios de acordo com as necessidades do cargo e responsabilidades do usuário;
- A revogação dos direitos de acesso deve ser realizada imediatamente após a saída do colaborador ou término do contrato.

Dessa forma, todas as contas de sistemas gerenciados pela UniFECAF devem seguir a regra de complexidade de senhas no mentor web e contas Google.

5.2 Gestão de Ativos

Identificar, classificar e proteger os ativos de informação relevantes, incluindo hardware, software, redes e dados durante todo o seu ciclo de vida.

- Estabelecer procedimentos abrangentes para o ciclo de vida dos ativos tecnológicos, incluindo sua disponibilização, utilização, devolução e descarte seguro;
    - Estabelecer um processo de avaliação e homologação, por parte da Segurança da Informação, de todo dispositivo, Sistema Operacional e software a ser implementado no ambiente da UniFECAF;
- Classificar as informações de acordo com seu nível de sensibilidade, atribuindo categorias ou níveis de classificação adequados;
    - Definir regras claras para o tratamento da informação com base em sua classificação;
    - Estabelecer medidas de proteção apropriadas para cada categoria de informação, considerando controles de acesso, criptografia, segregação de redes, entre outros, de acordo com sua classificação;

    - Realizar revisões periódicas na classificação de informações para garantir sua relevância e atualização, especialmente diante de mudanças nos requisitos de negócios ou regulatórios;
- Manter inventários atualizados dos ativos de informação, incluindo sua classificação, propriedade, responsabilidade e localização, a fim de facilitar a gestão e o monitoramento adequados;
- Implementar controles para que a informação da UniFECAF e de seus clientes, alunos e corpo docente, seja acessada somente através dos dispositivos homologados.

5.3 Política de Uso Aceitável

Promover o uso adequado dos recursos de tecnologia da informação da UniFECAF por parte dos colaboradores, prestadores de serviços e outras partes autorizadas.

- Estabelecer uma política clara de uso aceitável dos recursos de tecnologia da informação, incluindo o uso apropriado da Internet, redes sociais, e-mail e dispositivos móveis;
- Informar os colaboradores sobre as práticas aceitáveis e proibidas em relação ao uso de sistemas e informações confidenciais e dados pessoais;
- Monitorar o cumprimento da política de uso aceitável e tomar medidas corretivas quando necessário.

5.4 Gestão de Vulnerabilidades

Garantir que a empresa esteja ciente das vulnerabilidades e tome as medidas necessárias para reduzir ou eliminar os riscos associados a essas vulnerabilidades através da identificação, avaliação e mitigação as vulnerabilidades existentes nos sistemas, redes e aplicativos da UniFECAF.

- Realizar avaliações regulares de vulnerabilidades em sistemas, redes e aplicativos, utilizando ferramentas adequadas;
- Priorizar e remediar as vulnerabilidades identificadas de acordo com sua criticidade e impacto potencial;
- Implementar atualizações de segurança e patches de software de forma oportuna para mitigar as vulnerabilidades conhecidas.

5.5 Gerenciamento de Incidentes de Segurança

Estabelecer controles para identificar, relatar e responder a incidentes de segurança de forma eficaz e oportuna:

- Deve ser estabelecido um processo para identificar, relatar e responder a incidentes de segurança;
    - Definir um processo de gerenciamento de incidentes de segurança envolvendo fornecedores, estabelecendo responsabilidades claras e procedimentos para notificação, resposta e solução de incidentes;

- Conscientizar os colaboradores sobre a importância de relatar imediatamente quaisquer incidentes de segurança ou suspeitas de violações de dados;
- Realizar testes regulares de incidentes de segurança para avaliar a eficácia dos planos de resposta e identificar áreas de melhoria;
- Promover o aprendizado e aprimoramento dos controles por meio da análise dos incidentes de segurança da informação.

5.6 Gestão da Continuidade de Negócio

Garantir a disponibilidade dos serviços em caso de interrupções, como falhas de infraestrutura, desastres naturais ou ataques cibernéticos.

- Devem ser desenvolvidos e testados planos de continuidade de negócios para garantir a disponibilidade dos serviços da UniFECAF respeitando os SLAs acordados com os clientes em caso de cenários de interrupção como: falhas de infraestrutura, desastres naturais ou ataques cibernéticos;
- Os Planos de Continuidade de Negócios devem contemplar estratégias alinhadas com os objetivos de negócio da UniFECAF, definidas através dos BIAs.

5.7 Gestão de Backups e Restore

Garantir a disponibilidade e a integridade das informações críticas da UniFECAF, a recuperação de dados em caso de falhas ou desastres e a conformidade com as regulamentações aplicáveis.

- A UniFECAF estabelece procedimento específico que garante a cópia de maneira segura e por consequência a recuperação da informação quando necessário.
- Para garantir que este processo seja executado e utilizado existe um documento específico “Cópias de Segurança (Backup) e Recuperação (Restore)” com as diretrizes específicas para cópia e recuperação executados no processo de Backup.

5.8 Gestão de Fornecedores

Estabelecer um processo estruturado e eficiente para a gestão de fornecedores, a fim de garantir a segurança da informação e a conformidade com requisitos relevantes.

- Realizar uma avaliação criteriosa dos fornecedores em relação à segurança da informação, incluindo sua capacidade de proteger informações confidenciais e aderir a padrões de segurança reconhecidos;
- Estabelecer critérios claros para seleção de fornecedores, considerando sua experiência, reputação, histórico de segurança da informação e capacidade de atender aos requisitos específicos da organização;
- Incluir cláusulas contratuais que estipulem obrigações de segurança da informação, confidencialidade e conformidade regulatória por parte dos fornecedores;

5.9 Segurança Física

Implementar medidas de segurança física para proteger os ativos de informação contra acesso não autorizado, danos e perdas.

- Deve ser estabelecida uma política de controle de acesso físico às instalações da UniFECAF, garantindo que apenas pessoas autorizadas tenham acesso aos ambientes onde os dados são processados e armazenados;
- Deve ser implementado monitoramento e medidas de segurança física adequadas para proteger os ativos de informação contra ameaças físicas;
- As áreas de trabalho devem ser organizadas de forma a prevenir a visualização e acesso não autorizados a informações confidenciais.

5.10 Trabalho remoto

Assegurar que os colaboradores da empresa UniFECAF possam desempenhar suas atividades remotamente de forma segura, em conformidade com os requisitos de segurança estabelecidos pela organização.

- Implementar uma política que estabeleça diretrizes para garantir a segurança no trabalho remoto, incluindo a proteção de informações confidenciais e a aderência aos padrões de segurança da empresa;
- Implementar controles tecnológicos para estabelecer conexões remotas seguras, tais como o uso de VPN (Rede Virtual Privada), autenticação de dois fatores e criptografia de dados;
- Estabelecer requisitos de segurança para os dispositivos utilizados no trabalho remoto, como a instalação de softwares de segurança, atualizações regulares e proteção contra malware;
- Definir diretrizes claras para o armazenamento e compartilhamento de informações durante o trabalho remoto, incluindo o uso de soluções de armazenamento em nuvem seguras e a restrição de acesso a dados confidenciais;
- Realizar avaliação regular dos riscos associados ao trabalho remoto, identificando ameaças emergentes e implementando medidas de mitigação adequadas;
- Promover a conscientização e a educação dos colaboradores sobre boas práticas de segurança no trabalho remoto, por meio de treinamentos e comunicações periódicas;
- Estabelecer procedimentos claros para a gestão de incidentes de segurança durante o trabalho remoto, incluindo a notificação imediata de violações de segurança e ações corretivas apropriadas;

- Realizar revisões periódicas dos controles de segurança relacionados ao trabalho remoto, a fim de garantir sua eficácia contínua e identificar oportunidades de melhoria.

5.11 Gestão de Riscos

Identificar, avaliar, tratar e monitorar os riscos relacionados à segurança da informação, a fim de minimizar a probabilidade e o impacto de incidentes de segurança.

- Realizar uma avaliação de riscos de segurança da informação de forma regular e sistemática, considerando os ativos de informação, as ameaças e as vulnerabilidades relevantes para a UniFECAF;
- Documentar e revisar os resultados da avaliação de riscos, identificando as medidas de mitigação apropriadas para cada risco identificado;
- Implementar controles de segurança adequados para tratar os riscos identificados, considerando a eficácia, a viabilidade e o custo-benefício das medidas de mitigação;
- Monitorar continuamente os riscos identificados, revisando e atualizando a avaliação de riscos conforme necessário, especialmente diante de mudanças nos ambientes operacionais ou nas ameaças;
- Promover a conscientização sobre gestão de riscos entre os colaboradores, fornecendo treinamentos e orientações para ajudá-los a identificar e reportar potenciais riscos de segurança da informação.

6. Conscientização e Treinamento

A UniFECAF promoverá programas de conscientização e treinamento em Segurança da Informação aos colaboradoreso a fim de garantir a compreensão dos riscos e a adoção de práticas seguras no ambiente de trabalho.

Esta política de segurança da informação é de responsabilidade de todos os colaboradores da UniFECAF e seu cumprimento é fundamental para garantir a proteção das informações confidenciais dos clientes e a reputação da empresa.

7. Melhoria Contínua do SGSI

Esta política e todos os elementos que compõe o SGSI, deverão ser revisados em periodicidade máxima de 12 meses ou sempre que houver mudanças relevantes em seu escopo, a fim de garantir sua eficácia contínua e alinhamento com os objetivos de negócio da UniFECAF.