Tipo	Código
Política	**PL FIEB.003**
Título	Versão
Segurança da Informação do Sistema FIEB	**04**

1. Introdução

A Política de Segurança da Informação é uma declaração formal do Sistema FIEB a respeito do seu compromisso com a proteção dos ativos de informação de sua propriedade ou sob sua guarda. Deve, portanto, ser cumprida pelas partes interessadas pertinentes: Diretoria da FIEB, Diretoria do CIEB, sindicatos, conselhos das entidades (FIEB, SESI/DR/BA, SENAI/DR/BA e IEL/BA), força de trabalho, fornecedores, parceiros e por qualquer pessoa física ou jurídica vinculada de alguma forma ao Sistema FIEB, que tenham acesso a seus dados ou informações.

Esta Política de Segurança da Informação foi elaborada pelas Comissões de Segurança da Informação do Sistema FIEB, com base nas normas técnicas ABNT NBR ISO/IEC 27001:2013 e 27002:2013, de acordo com a legislação vigente, realidade e requisitos de negócio das entidades.

> *"A segurança da informação é alcançada pela implementação de um conjunto adequado de controles, incluindo políticas, processos, procedimentos, estrutura organizacional e funções de software e hardware. Estes controles precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados, quando necessário para assegurar que os objetivos do negócio e a segurança da informação da organização sejam atendidos. "*
>
> *ABNT NBR ISO/IEC 27002:2013*

2. Objetivos

Definir e padronizar o uso, tratamento, controle e proteção das informações que possam causar impactos no seu desempenho financeiro, na sua participação no mercado, na sua imagem, agregando valor à operação e eficiência na prestação de serviços ou no seu relacionamento com as partes interessadas, contemplando os seguintes objetivos específicos:

- Definir o escopo da segurança da informação do Sistema FIEB;
- Definir as responsabilidades na gestão da segurança da informação;
- Definir as responsabilidades das partes interessadas pertinentes na preservação da segurança da informação;
- Orientar as ações de segurança da informação das Entidades para reduzir riscos e

garantir a integridade, confidencialidade e a disponibilidade da informação;

- Manter o Sistema de Gestão de Segurança da Informação no âmbito do Sistema FIEB;
- Servir de referência para auditorias, apuração e avaliação de responsabilidades.

3. Escopo

Esta Política considera a abrangência da segurança da informação nos aspectos físico, lógico e comportamental, preservando a confidencialidade, integridade e disponibilidade das informações do Sistema FIEB.

4. Definições

Para compreensão deste documento adotam-se os seguintes termos e definições:

a) Alta administração:

Diretoria da FIEB, Diretoria do CIEB, sindicatos, conselhos das entidades (SESI/DR/BA, SENAI/DR/BA e IEL/BA).

b) Ameaça:

Causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização.

c) Demais usuários:

Grupo formado pelos membros dos Sindicatos, Conselhos Temáticos ou outras pessoas físicas ou jurídicas que utilizam os recursos de Tecnologia da Informação do Sistema FIEB.

d) Força de trabalho do Sistema FIEB:

Pessoas que compõem uma organização e que contribuem para consecução de suas estratégias, objetivos e metas ou realizam atividades de aprendizagem, tais como empregados em tempo integral ou parcial, temporários, estagiários, autônomos e contratados de terceiros que trabalham sob a coordenação direta da organização.

Colaborador: todo e qualquer empregado do Sistema FIEB.

Líderes: grupo formado por coordenadores, gerentes, superintendentes e diretores.

Multiplicador/Facilitador: grupo composto por colaboradores efetivos, responsáveis por disseminar esta política e apoiar no seu cumprimento.

Terceiros: grupo composto por profissionais, vinculados a empresas contratadas ou

não, fornecedores, prestadores de serviços, parceiros e clientes que possuam acesso a informações do Sistema FIEB.

e) Gerência de Tecnologia da Informação (GTI):

Área responsável pela gestão dos recursos computacionais que suportam as atividades das entidades do Sistema FIEB.

f) Incidente de segurança da informação:

Evento ou série de eventos indesejados ou inesperados, que tenham grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação. Uma ameaça que se concretiza gera um incidente.

g) Informação:

Conjunto de dados, imagens, textos e quaisquer outras formas de representação dotadas de significado dentro de um contexto.

h) Informação sensível ou crítica:

Toda e qualquer informação cujo comprometimento possa causar perda de vantagem competitiva, dano ou prejuízo ao negócio ou à imagem da organização.

i) Monitoramento:

Acompanhamento e avaliação de dados e processos com objetivo específico de proteger o negócio, seus ativos e pessoas contra ameaças, prevenindo ataques ou outras manifestações que possam resultar em prejuízo para organização.

j) Recursos de Tecnologia da Informação:

Referem-se a qualquer sistema de armazenamento ou processamento da informação, serviço ou infraestrutura, ou às instalações físicas que os abriguem, tais como: pen drives, smartphones, tablets, e-mail, planilhas, documentos, computadores, notebooks, equipamentos de rede, dentre outros.

k) Segurança da Informação (SI):

A informação é um ativo das organizações, ou seja, é um bem que possui valor e, portanto, deve ser protegida, independentemente de ser escrita ou impressa em papel, armazenada eletronicamente, transmitida pelo correio ou através de meios eletrônicos, mostrada em filmes ou falada em conversas. A segurança da informação é alcançada através da preservação da integridade, confidencialidade e disponibilidade da informação.

Integridade: é a garantia da preservação da informação e consistência dos dados ao longo do seu ciclo de vida.

Confidencialidade: é a garantia de sigilo, ou seja, a informação é acessível somente a pessoas autorizadas a terem acesso.

Disponibilidade: é a garantia de que a informação e os ativos associados estejam disponíveis para os usuários legítimos, sempre que necessário.

l) Sistema FIEB

Grupo de entidades composto por FIEB, CIEB, SESI/DR/BA, SENAI/DR/BA e IEL/BA.

m) Software malicioso ou *malware*:

Entende-se por software malicioso qualquer software que realiza ações nocivas aos sistemas, como vírus, *worm, ransonware* e afins.

n) Vírus:

Entende-se por vírus qualquer programa de computador que tem a capacidade de se reproduzir automaticamente, sem o conhecimento ou autorização do usuário e causar danos as informações ou sua disponibilidade.

o) Vulnerabilidade:

Fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças.

5. Papéis e responsabilidades

A Diretoria da FIEB, Diretoria do CIEB, sindicatos, conselhos das entidades (SESI/DR/BA, SENAI/DR/BA e IEL/BA), força de trabalho, fornecedores e parceiros têm responsabilidade sobre as informações que acessam e manipulam. A observância das diretrizes constantes nesta política, independe da existência de controles que, de forma total ou parcial, obriguem o seu cumprimento.

5.1. Comissões de Segurança da Informação

a) Propor e revisar a Política de Segurança da Informação e documentos relacionados (guias, padrões complementares, acordo de confidencialidade, dentre outros) sempre que necessário;

b) Viabilizar que as atividades desempenhadas pelas entidades sejam executadas em conformidade com a Política de Segurança da Informação vigente;

c) Avaliar violações à Política de Segurança da Informação e propor ações para tratá-las;

d) Propor ou avaliar a adequação de diretrizes, controles, metodologias e processos inerentes à segurança da informação, tais como análise/avaliação de riscos e classificação da

informação, dentre outros;

e) Avaliar o resultado de análises, auditorias e incidentes de segurança da informação e propor ações preventivas e/ou corretivas;

f) Assessorar auditorias para verificar o cumprimento da política, normas, procedimentos e outros documentos afins relacionados com a Segurança da Informação;

g) Propor capacitação em segurança da informação, definindo o conteúdo, periodicidade e público-alvo dos treinamentos;

h) Manter contato com entidades ou grupos externos relacionados à segurança da informação a fim de agregar melhorias à Política de Segurança da Informação;

i) Assessorar a alta administração nos assuntos relativos à segurança da informação.

Para desempenhar as atribuições listadas, as Comissões de Segurança da Informação devem se reunir regularmente, com frequência a ser definida pelos seus membros, podendo, por meio de convocação do coordenador, reunir-se extraordinariamente para tratar de assuntos específicos ou urgentes.

5.2. Coordenador de Segurança da Informação

a) Fornecer o embasamento técnico necessário às Comissões de Segurança da Informação, para subsidiar a tomada de decisão;

b) Coordenar a implantação dos controles e processos de segurança da informação aprovados pela alta administração;

c) Identificar fragilidades, exposição da informação e dos recursos de processamento da informação e ameaças significativas;

d) Manter registro de incidentes e fragilidades de segurança da informação para apresentação periódica as Comissões de Segurança da Informação;

e) Coordenar ações emergenciais de segurança da informação, que não possam aguardar uma reunião das Comissões de Segurança da Informação;

f) Realizar periodicamente análise crítica independente da segurança da informação, considerando inclusive auditorias realizadas, para avaliar a efetividade desta Política de Segurança da Informação e dos controles de segurança da informação adotados;

g) Articular-se com os multiplicadores de segurança da informação das unidades e áreas do Sistema FIEB, visando o cumprimento desta Política.

5.3. Diretoria da FIEB e do CIEB, sindicatos, Conselhos das entidades (SESI, SENAI e IEL), força de trabalho, fornecedores, clientes e parceiros com acesso às informações corporativas

a) Cumprir as determinações desta Política de Segurança da Informação, bem como seus respectivos documentos complementares;

b) Proteger a informação contra acesso não autorizado, divulgação, modificação, destruição ou interferência, em todo o seu ciclo de vida;

c) Notificar, com a maior brevidade possível, quaisquer incidentes, fragilidades ou falhas de segurança ao Coordenador de Segurança da Informação.

Convém destacar que fragilidades ou falhas de segurança não devem ser testadas pelos usuários, apenas notificadas quando percebidas. Da mesma forma, ações corretivas não devem ser adotadas por conta própria.

Adicionalmente, o cumprimento desta Política de Segurança da Informação faz parte das responsabilidades de trabalho e, a partir da sua publicação, deve constar nas cláusulas de contratos de trabalho e contratos com fornecedores em que suas disposições se aplicarem.

5.4. Líderes

a) Difundir a Política de Segurança da Informação e viabilizar, no âmbito de sua gestão, a educação, o treinamento e a conscientização sobre segurança da informação;

b) Identificar as necessidades de segurança da informação nos processos sob sua responsabilidade, inclusive propondo novas medidas de controle;

c) Validar as solicitações de acesso aos dados e sistemas de interesse para processos sob sua responsabilidade, revisando os acessos periodicamente.

5.5. Multiplicadores

a) Divulgar o conteúdo da política em sua Unidade/área aos atuais e novos colaboradores, através de palestras, ambientações, seminários, reuniões, campanhas educativas, mutirões, meios de comunicação, etc;

b) Apoiar no cumprimento da política e suas normas, assim como esclarecer as dúvidas relacionadas a este tema.

6. Acordo de Confidencialidade

Considera-se celebrado o acordo de confidencialidade com a força de trabalho a partir da publicação desta Política. Cláusulas referentes a garantia da segurança e confidencialidade da informação constam nos instrumentos celebrados com fornecedores e parceiros (tais como contratos, convênios, termos de cooperação, parcerias e de compromisso) observando-se que:

- O acordo de confidencialidade é valido durante todo o período de vigência do contrato e adicionalmente terá duração de 10 (dez) anos após o término da vigência ou obedecerá ao prazo que tiver sido especificamente definido no instrumento firmado;
- Em quaisquer outros casos, o prazo de validade do acordo de confidencialidade obedecerá a regulamentação que orienta a atividade específica, como: saúde, educação, propriedade intelectual, dentre outras.

7. Treinamento e conscientização em segurança da informação

Todos os colaboradores devem receber capacitação periódica em Segurança da Informação. Os líderes das áreas devem indicar a participação de seus colaboradores.

Para toda a força de trabalho são disponibilizadas as orientações de segurança necessárias.

8. Propriedade Intelectual

O respeito à propriedade intelectual está intimamente relacionado ao negócio do Sistema FIEB. As seguintes diretrizes devem ser observadas:

- A força de trabalho do Sistema FIEB deve respeitar o uso legal de propriedade intelectual de terceiros, incluindo softwares, livros, artigos, filmes, áudio, imagens, ou qualquer outro conteúdo sujeito à legislação de propriedade intelectual.
- Qualquer trabalho desenvolvido pela força de trabalho pertence ao Sistema FIEB, exceto, em casos de negociações específicas aprovadas pela alta administração, conforme a alçada.

9. Processos disciplinares

Violações a esta Política de Segurança da Informação e demais documentos complementares

sobre segurança da informação serão analisados pelo Coordenador de Segurança da Informação, superior imediato da área onde o fato ocorreu e pelas Comissões de Segurança da Informação, conforme a natureza, gravidade e impacto causado.

Poderá ser recomendada a instauração de sindicância para averiguação dos fatos, quando houver indícios de ocorrência de infração funcional, sem prejuízo responsabilização penal e civil do suposto infrator.

Concluída a apuração, conforme normas específicas das entidades do Sistema FIEB, e comprovada a ocorrência da infração, poderão ser aplicadas as penalidades previstas na legislação vigente e nos regulamentos internos, observada a proporcionalidade entre a infração e a sanção respectiva, e respeitado os primados da ampla defesa e do contraditório.

10.Documentos da política de segurança

A Política de Segurança da Informação do Sistema FIEB é complementada por diretrizes e documentos afins, considerados como parte integrante desta política e são, por delegação, assinados pelo Gerente de Tecnologia da Informação.