POLÍTICAS DE GESTÃO DA SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA

ÁREA PROPONENTE

1.1Gerência de Inovação e Processos – GEPRO

POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA

OBJETIVO

2.1 Esta Política se destina a orientar Dirigentes, Colaboradores e Fornecedores a executar suas atividades de maneira voltada para a Segurança da Informação e Cibernética de forma a proteger as informações corporativas e demais ativos de informação da FUSESC, apresentando diretrizes e políticas aprovados pelo Conselho Deliberativo.

CLASSIFICAÇÃO DA INFORMAÇÃO

3.1 Esta Política é de acesso Confidencial.

3.2 As informações criadas, manuseadas, armazenadas, transportadas ou custodiadas no âmbito da FUSESC serão classificadas em quatro categorias de acordo com o nível de confidencialidade:

3.2.1 Informações de acesso Público: Informações que podem ser acessadas pelo Público em Geral.

3.2.2 Informações de acesso Interno: Informações que podem ser acessadas somente por Dirigentes e Colaboradores da FUSESC.

3.2.3 Informações de acesso Confidencial: Informações que podem ser acessadas por Dirigentes, Colaboradores, Participantes, Assistidos, Patrocinadoras e Fornecedores mediante disponibilização direta de conteúdo e/ou acesso à informação destinada especificamente para estes públicos.

3.2.4 Informações de acesso Restrito: Informações que podem ser acessadas somente por Dirigentes e pessoas físicas ou jurídicas diretamente autorizadas.

3.3 A classificação a que se refere o item 3.2.4 poderá ser declarada a qualquer momento, de forma expressa e motivada, por qualquer Diretor ou por decisão dos Conselhos Fiscal ou Deliberativo.

3.4 Todos os Colaboradores devem ser capazes de identificar a classificação de segurança atribuída a uma informação tratada pela FUSESC e, a partir dela, conhecer as restrições de acesso e de divulgação associadas.

3.5 Todo documento eletrônico institucional deve ser armazenado nos servidores de arquivos da rede corporativa ou em ferramentas de colaboração corporativa homologadas pela GEPRO.

3.6 Se o documento não for eletrônico, deve ser mantido em local que preserve a segurança das informações.

3.7 No descarte de informações institucionais, devem ser observados: a temporalidade prevista na legislação, as políticas, as normas, os procedimentos internos e a classificação atribuída pela legislação à informação.

PÚBLICO ALVO

4.1 São público-alvo desta Política:

4.1.1 Em relação à FUSESC: seus Participantes, Assistidos, Dirigentes, Colaboradores, Patrocinadoras e Fornecedores.

4.1.2 Pessoas físicas ou jurídicas que não se enquadram na qualificação do item anterior e mantenham relacionamento com a FUSESC.

4.1.3 Público em geral.

GLOSSÁRIO

5.1 **Segurança da Informação e Cibernética:** conjunto de conceitos, técnicas, estratégias e tecnologia, as quais visam proteger os ativos de informação, bem como redes, computadores e sistemas de ataques que possam causar danos ou acesso não autorizado.

5.2 **Dado ou informação:** são todos os dados que lidos isoladamente ou em conjunto representam às atividades desenvolvidas pela FUSESC na execução dos processos de negócio.

5.3 **Incidente:** qualquer ocorrência que realmente ou potencialmente comprometa a confidencialidade, integridade ou disponibilidade de um sistema de informação ou a informação que o sistema processa, armazena ou transmite ou que constitui uma violação ou ameaça iminente de violação de políticas de segurança ou procedimentos de segurança.

5.4 **Vulnerabilidades:** brecha sistêmica ou em processos que permite ataque de exploração ou violação à segurança da informação de uma aplicação ou rede.

5.5 **Riscos de segurança da informação:** são os riscos de ataques cibernéticos, oriundos de *malware*, técnicas de engenharia social, invasões, ataques de rede, fraudes externas, entre outros, que possam expor dados, redes e sistemas da FUSESC.

DOS PRINCÍPIOS

6.1 São princípios desta Política:

6.1.1 A legalidade, a impessoalidade, a moralidade, a publicidade, a eficiência e a ética na proteção do ativo de informação;

6.1.2 A preservação da disponibilidade, da integridade, da autenticidade e do sigilo, quando aplicável, do ativo de informação;

6.1.3 A responsabilização individual na utilização indevida dos ativos da informação;

6.1.4 O tratamento e a publicidade de informações de acordo com seu nível de classificação institucional.

DISPOSIÇÕES GERAIS

7.1 Esta Política deve ser aplicada ao ambiente corporativo da FUSESC independente do regime de trabalho, seja presencial ou teletrabalho e difundida por um processo permanente de conscientização a todos os Colaboradores e a todos que possuam acesso aos recursos de Tecnologia da Informação.

7.2 Os controles relacionados à Segurança da Informação e Cibernética aplicados no ambiente presencial devem ser os mesmos aplicados ao ambiente de teletrabalho, salvo algum item de segurança adicional que a GEPRO julgue necessário implementar.

7.3 Os Colaboradores devem conhecer e zelar pelo cumprimento desta.

7.4 Os usuários dos recursos de Tecnologia da Informação são responsáveis pela segurança dos recursos e pelos processos que estejam sob sua responsabilidade e uso.

7.5 Os recursos de Tecnologia da Informação disponibilizados pela FUSESC devem ser utilizados estritamente para fins institucionais, sendo vedado, a qualquer Colaborador que tenham acesso a tais recursos, sua utilização para fins diversos daqueles para os quais foram concebidos, dentre eles, o uso para:

7.5.1 Perpetuar qualquer ação que possa comprometer a integridade, a disponibilidade, a autenticidade e o sigilo, quando aplicável, das informações criadas, manuseadas, armazenadas, transportadas, descartadas ou custodiadas pela FUSESC;

7.5.2 Fins pessoais ou de terceiros que violem as normas de direito autoral, de propriedade industrial e demais normas ou leis que venham dispor sobre esta temática;

7.5.3 Veiculação de opiniões sexuais, racistas, político-partidárias ou religiosas;

7.5.4 Perpetrar ações que venham a caluniar, difamar e injuriar qualquer pessoa física ou jurídica;

7.5.5 Expressar opiniões que venham a prejudicar direta ou indiretamente a imagem da FUSESC;

7.5.6 Entretenimento.

TRATAMENTO DAS INFORMAÇÕES

8.1 Todas as informações criadas, manuseadas, armazenadas ou transportadas pelos Colaboradores no exercício de suas atividades são de propriedade da FUSESC e devem ser protegidas segundo as diretrizes descritas nesta documentação e nas demais normas jurídicas que disponham sobre direito autoral, propriedade industrial e sigilo das informações, incluindo a proteção jurídica dos respectivos sistemas que as armazenam.

8.2 Nos casos de cessão a terceiros do acesso as informações pertencentes à FUSESC, a GEPRO deve providenciar previamente perante o cessionário a celebração do instrumento jurídico adequado à formalização da cessão do direito de uso dessas informações em favor do interessado, estendendo-se a este último, conforme o caso, a obrigação de manter o sigilo das informações. O instrumento jurídico a ser elaborado, e referido, deve ser submetido à análise jurídica prévia.

8.3 Nos casos de obtenção de informação de acesso restrito pertencente a terceiros, a GEPRO deve previamente providenciar perante o fornecedor das informações a celebração do instrumento jurídico adequado à formalização da cessão do direito de uso dessas informações em favor da FUSESC, estendendo-se, conforme o caso, a obrigação de manter o sigilo das informações. O instrumento jurídico a ser elaborado, e referido, deve ser submetido à análise jurídica prévia.

REGISTRO, RESPOSTA E TRATAMENTO DE INCIDENTES

9.1 Todo Colaborador, ao tomar conhecimento ou suspeitar da possibilidade de ocorrência de qualquer incidente de segurança da informação e comunicações, deve notificar o fato imediatamente à GEPRO para as providências cabíveis.

9.2 Cabe à GEPRO verificar o impacto causado pelo incidente cibernético, avaliar a criticidade de segurança, aplicar as medidas de contenção e erradicação.

9.3 Os incidentes devem ser registrados de forma a criar uma base de conhecimento para que os mesmos erros não voltem a acontecer, especificando quais foram os procedimentos de respostas utilizadas para contorná-los.

9.4 Em casos de incidentes relacionados a dados pessoais e dados sensíveis, a situação dever ser encaminhada para análise do Encarregados de Dados da FUSESC para avaliar se houve risco ou dano relevante aos titulares dos dados impactados.

9.5 A GEPRO deve estabelecer controles e procedimentos relacionados à segurança da informação e cibernética, tais como: autenticação, criptografia, proteção contra softwares maliciosos, detecção de vulnerabilidades, dentre outros.

9.6 Cabe à GEPRO estabelecer critérios para classificação dos incidentes identificados.

9.7 Os incidentes decorrentes do relacionamento com prestadores de serviços e terceiros devem seguir as diretrizes e os procedimentos estabelecidos nesta Política ou em Instruções Normativas internas.

CONTROLES DE ACESSO

10.1 Todo Colaborador da FUSESC deve ter no ambiente da rede corporativa uma conta de identificação de usuário, de caráter intransferível, sendo pré-requisito para sua concessão o conhecimento quanto ao Compromisso de Sigilo, no qual a autorização, o acesso e o uso da informação e dos recursos de tecnologia devem ser controlados e limitados à necessidade do cumprimento das atribuições funcionais do usuário, sendo necessária prévia autorização formal da GEPRO para qualquer finalidade.

10.2 Contas de acesso à rede devem ser individuais e não-compartilhadas, salvo em situações especiais em que a GEPRO julgar necessário dentro prazos pré-determinados e controlados.

10.3 Eventuais mudanças nas atribuições funcionais dos Colaboradores da FUSESC que ensejam na necessidade de ampliação ou restrição de acessos

devem ser comunicadas à GEPRO via chamado técnico de serviço para se proceder com a atualização das credenciais de acesso de acordo com a nova atribuição do Colaborador.

10.4 O acesso aos recursos de Tecnologia da Informação sob responsabilidade da FUSESC, próprios ou cedidos temporariamente, poderá ser concedido a Colaboradores ou a terceiros, em conformidade com esta Política.

10.5 O acesso físico às instalações da FUSESC deverá ser objeto de monitoração com o objetivo de garantir a segurança dos Dirigentes e Colaboradores, bem como à proteção dos seus ativos de informação.

10.6 As senhas de acesso são pessoais e intransferíveis, devendo ser alteradas periodicamente, não podendo ser compartilhadas, divulgadas a terceiros ou a outros Colaboradores da FUSESC, anotadas em papel ou em sistema visível ou de acesso não protegido, mantida, em qualquer caso, a responsabilidade pelo uso da senha pelo seu titular.

10.7 Somente será permitida a conexão de novos computadores à rede da FUSESC após solicitação dos gestores das áreas e aprovação da GEPRO. Todos os computadores conectados devem obedecer aos procedimentos padronizados de segurança estabelecidos pela FUSESC. Deve ser facultado o acesso do(s) administrador(es) de rede da FUSESC a todos os equipamentos ligados a esta, possibilitando a realização de procedimentos de auditoria, controle e segurança necessários.

10.8 É proibida toda e qualquer tentativa deliberada de retirar o acesso à rede ou a qualquer computador da FUSESC ou de prejudicar o seu rendimento. São procedimentos considerados graves:

10.8.1 Criar ou propagar vírus, danificar serviços e arquivos;

10.8.2 Destruir ou estragar intencionalmente equipamentos, *software* ou dados pertencentes à FUSESC ou a outros usuários;

10.8.3 Obter acesso a qualquer recurso não-autorizado;

10.8.4 Obter acesso não-autorizado aos sistemas.

GESTÃO DE RISCOS

11.1 A FUSESC deverá analisar, elaborar e manter processos de Gestão de Riscos, com o objetivo de minimizar possíveis impactos associados aos recursos tecnológicos, onde o processo criado deve possibilitar a seleção e priorização dos recursos a serem protegidos, e a definição e controle para a identificação e tratamento de possíveis problemas de segurança.

11.2 Os recursos tecnológicos disponibilizados para a criação, manuseio, armazenamento, transporte e descarte da informação na FUSESC devem dispor de mecanismos que minimizem os riscos inerentes a problemas de segurança, com o objetivo de evitar ocorrências de incidentes, acidentais ou intencionais, que afetem os princípios de integridade, disponibilidade, autenticidade e sigilo, quando aplicável, das informações.

11.3 Os recursos tecnológicos utilizados pela FUSESC devem ser previamente homologados, identificados individualmente e inventariados, além de possuir documentação mínima e atualizada para o seu uso.

11.4 Os riscos de segurança da informação devem ser monitorados e analisados por meio de soluções tecnológicas automatizadas.

11.5 Riscos possivelmente causadores de eventos que possam interromper as atividades da Entidade ou gerar uma crise institucional devem observar cenários de contingência que permitam a continuidade das atividades em níveis aceitáveis. Os cenários de contingência devem ser validados por meio dos testes previstos na Política de Gestão de Continuidade de Negócios e Gerenciamento de Crise e em Instruções Normativas internas.

AUDITORIA E CONFORMIDADE

12.1 O uso dos recursos tecnológicos disponibilizados pela FUSESC é passível de monitoramento, cabendo à GEPRO implantar e manter mecanismos que permitam a rastreabilidade desse uso.

12.2 É obrigatória a identificação física, pessoal e intransferível, do Colaborador e de todos que possuam acesso aos recursos tecnológicos, incluindo visitantes, a ser efetuada pela GEPRO, a qual qualificará os responsáveis por todas as ações praticadas.

12.3 A entrada e a saída de recursos tecnológicos das dependências físicas da FUSESC devem ser autorizadas e registradas pela GEPRO.

12.4 A FUSESC não autoriza casos em que seus Colaboradores ou terceiros utilizem *software* ou *hardware* não homologados pela GEPRO.

12.5 Devem ser criados, nos ativos tecnológicos, controles técnicos que permitam a realização de auditorias.

UTILIZAÇÃO DO CORREIO ELETRÔNICO

13.1 A conta de correio eletrônico corporativa disponibilizada ao Colaborador da FUSESC é pessoal e intransferível, sendo seu titular o único responsável pelas ações e danos causados à Instituição por meio de seu uso.

13.2 O correio eletrônico deve ser utilizado para atividades afeitas ao trabalho,

ao desenvolvimento profissional pessoal e a manutenção da conformidade das condições para atuação em sua função/cargo na FUSESC.

ACESSO À INTERNET

14.1 O acesso à *internet* é um serviço disponibilizado aos Colaboradores pela FUSESC e deve ser utilizado para atividades afeitas ao trabalho, ao desenvolvimento profissional pessoal e a manutenção da conformidade das condições para atuação em sua função/cargo na FUSESC.

UTILIZAÇÃO DE DISPOSITIVOS MÓVEIS

15.1 A eventual utilização de dispositivos móveis de propriedade da FUSESC será restrita à execução de atividades relacionadas às finalidades corporativas

15.1.1 Os dispositivos constantes no item 15.1 serão monitorados nos mesmos moldes dos computadores/notebooks disponibilizados pela FUSESC.

15.2 A utilização de dispositivos móveis particulares será permitida observadas as seguintes condições:

15.2.1 Os Colaboradores deverão comunicar à Gerência de Inovação e Processos sua opção por utilizar seus dispositivos pessoais (BYOD – bring your own device), como smartphones e tablets, para acesso à rede corporativa, sistemas internos e bancos de dados, observando as condições de uso estabelecidas pela FUSESC.

15.2.2 Caberá à GEPRO implantar soluções para prevenir incidentes de segurança e possíveis violações à Política de Segurança e Cibernética.

15.2.3 A GEPRO auditará o dispositivo, e poderá instalar ferramentas de monitoramento e remoção remota de informações (para caso de roubo ou perda do dispositivo).

15.2.4 Os dispositivos BYOD devem conter configurações de segurança mínimas estabelecias pela GEPRO.

MONITORAMENTO

16.1 Caberá à GEPRO a elaboração e implementação de ferramentas digitais para controle e monitoramento referente ao acesso à informação, trânsito de dados, informações e conteúdos em meio digital no âmbito da FUSESC.

16.2 Caberá a DIREX, em conjunto ou isoladamente, tomar as decisões de acesso detalhado a informações e conteúdo abrangidos por esta Política, podendo utilizar os relatórios de monitoramento e controle digitais produzidos

pela GEPRO.

ATUALIZAÇÕES E CORREÇÕES DE SEGURANÇA

17.1 As atualizações de segurança disponibilizadas pelos fornecedores de recursos computacionais devem ser realizadas pela GEPRO, observando a estabilidade, compatibilidade, licenciamento, custo e aplicabilidade.

17.2 Caberá à GEPRO preparar um ambiente de homologação para receber as atualizações ou correções de segurança, se assim julgar necessário.

PENALIDADES

18.1 A utilização indevida de recursos e informações e a violação desta Política poderão ser submetidas ao Comitê de Ética na forma do Código de Conduta e Ética da FUSESC, sem prejuízo de sanções disciplinares.

ORIENTAÇÕES GERAIS PARA PARCEIROS E FORNECEDORES

19.1 Sem prejuízo das condições contratuais e das condutas de boas práticas esperadas, o parceiro ou fornecedor deve observar as seguintes orientações:

19.1.1 Proteja a informação recebida por força do contrato contra a intercepção, cópia, modificação não autorizada, indisponibilidade, desvio e destruição.

19.1.2 Mantenha programa de educação, treinamento e conscientização sobre segurança da informação para funcionários que tiveram acesso às informações corporativas.

19.1.3 Comunique quaisquer anormalidades detectadas que possam comprometer a segurança das informações ou serviço e outras ocorrências relevantes.

19.1.4 Em caso de contratação de serviços de processamento e armazenamento de dados e de computação em nuvem devem ser adotadas práticas de governança corporativas de modo a avaliar os riscos a que estejam expostas as informações objeto da contratação, bem como estabelecer contratualmente na medida do possível mecanismos de controle de qualidade e de capacidade técnica do fornecedor.

PAPÉIS E RESPONSABILIDADES

20.1 Do Conselho Deliberativo:

20.1.1 Deliberar sobre esta Política e respectivas revisões.

20.2 Da Diretoria Executiva:

20.2.1 Instruir a execução das atividades por intermédio de normativos internos afeitos à Segurança da Informação e Cibernética.
20.2.2 Proporcionar capacitação adequada dos Colaboradores que compõem a estrutura de gerenciamento de segurança cibernética, acerca das políticas, dos planos e dos controles.

20.3 Do Diretor Financeiro e Administrativo:

20.3.1 Supervisionar o desenvolvimento e a implementação da estrutura de gerenciamento de segurança cibernética.
20.3.2 Supervisionar as atividades da área técnica responsável pelo monitoramento do acesso à informação.

20.4 Da Gerência de Inovação e Processos - GEPRO:

20.4.1. Propor políticas, planos, manuais e controles para o gerenciamento de segurança da informação e cibernética;
20.4.2 Definir e acompanhar indicadores de gestão da segurança da informação e cibernética;
20.4.3 Executar a devida correção tempestiva das deficiências das estruturas de gerenciamento de segurança da informação e cibernética;
20.4.4 Prestar apoio Diretoria Executiva, nos assuntos relacionados à gestão de segurança da informação e cibernética;
20.4.5 Executar ações de disseminação da cultura de gerenciamento de segurança da informação e cibernética.

DISPOSIÇÕES FINAIS

21.1 As normas constantes nesta devem servir como diretriz institucional para elaboração das demais normas relacionadas ao uso de recursos tecnológicos e ao desenvolvimento dos procedimentos operacionais e de segurança técnica.

21.2 Os Colaboradores da FUSESC devem reportar à GEPRO os incidentes que potencialmente afetem a segurança dos recursos tecnológicos ou que impliquem no descumprimento de políticas ou diretrizes existentes.

21.3 Em casos de risco ou quebra de segurança da informação, a GEPRO deverá adotar as providências necessárias à correção do incidente, podendo, inclusive, determinar a restrição temporária do acesso às informações e aos recursos de tecnologia da informação.

ATUALIZAÇÕES DESTA POLÍTICA

22.1 A FUSESC deve, no mínimo a cada 02 (dois) anos, promover a revisão das

suas políticas de segurança e, a qualquer tempo, atualizações que se fizerem necessárias, decorrentes de mudanças na legislação ou desenvolvimento de novos processos de trabalho.

22.2 Os controles de atualizações dos documentos formais de governança da FUSESC são registrados em sistema eletrônico.

22.3 Os casos omissos devem ser dirimidos pelo Conselho Deliberativo.

CONTROLE DE VERSIONAMENTO:

Data da Aprovação	25/07/2024
Início da Vigência	25/07/2024
Processo Decisório Nº	002867/2024
Periodicidade de Revisão	02 anos
Ata de Aprovação CODEL	453, de 25/07/2024