HIERARQUIA DOS DOCUMENTOS

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

ECONOMUS

1. POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

1.1. Objetivo

1.1.1. Estabelecer diretrizes e definir o tratamento que deve ser dado às informações geradas, armazenadas, processadas, transitadas e transmitidas no Economus, bem como orientar o comportamento dos empregados em relação à promoção da segurança da informação e proteção dos ativos da Entidade.

1.2. Fundamentação Legal

1.2.1. Em linha com a legislação vigente, é imprescindível uma gestão permanente e pervasiva da Segurança da Informação a fim de promover a manutenção de um nível de risco adequado e o alcance dos seus objetivos como uma Entidade de Previdência Complementar, assim como, é parte fundamental do seu arcabouço de controles internos considerando seu porte e complexidade

1.3. Abrangência

1.3.1. Esta Política aplica-se a:

a) Conselheiros - membros dos Conselhos Deliberativo e Fiscal do Economus;

b) Dirigentes - membros da Diretoria Executiva do Economus;

c) Empregados - empregados do quadro próprio do Patrocinador;

d) Cedidos - funcionários do Patrocinador que prestam serviço no Economus por meio de convênio de cessão;

e) Colaboradores - Terceirizados, Consultores, Estagiários e Jovens Aprendizes;

f) Fornecedores e Prestadores de serviço e seus empregados - enquanto prestarem serviços ao Economus.

1.4. Responsável

1.4.1. A área de Riscos e Controles Internos é a gestora da Política de Segurança da Informação.

1.5. Diretrizes Gerais

1.5.1. Tratamos a informação, na gestão institucional, como ativo.

1.5.2. Garantimos na gestão da informação a confidencialidade, a disponibilidade e a integridade em todos os processos em que há tratamento da informação, sejam eles informatizados ou não, por meio de mecanismos de proteção.

1.5.3. Protegemos os ativos de informação de forma proporcional ao seu grau de importância para o Economus, a qual deve ser aferida por meio da classificação da informação.

1.5.4. Responsabilizamos o custodiante das informações pelo zelo na preservação e confidencialidade enquanto estas estiverem sob sua guarda.

1.5.5. Protegemos nossos ativos de informação contra uso inadequado, perdas, divulgações ou modificações não desejadas.

1.5.6. Concedemos acesso à informação por meio de critérios definidos por funções e atribuições de cargos ou serviços prestados, a quem de direito, obedecendo aos princípios de segregação de função. Tal acesso deve ser limitado apenas ao necessário para a realização das tarefas designadas ao usuário.

1.5.7. Responsabilizamos o gestor da informação na definição e autorização das permissões de acesso à mesma, incluindo ou excluindo pessoas da lista de acessos, ou mesmo, alterando o nível de acesso de uma pessoa à informação.

1.5.8. Classificamos toda informação, quando criada no Economus ou recebida de fonte externa, conforme seu grau de sigilo, tendo como base o eventual impacto negativo decorrente de acesso ou divulgação não autorizada, de acordo com os níveis descritos abaixo:

a) CONFIDENCIAL (#CONFIDENCIAL): é uma informação crítica para os negócios do Economus ou por determinação legal, como por exemplo, dados pessoais. A divulgação não autorizada dessa informação pode causar impactos de ordem financeira, de imagem, operacional ou, ainda, sanções administrativas, civis e criminais ao Instituto. É restrita a um grupo específico de pessoas devidamente autorizadas. Deve ser acessada com restrições por colaboradores, fornecedores e prestadores de serviços do Economus, apenas sob um contrato vigente e assinatura de Termo de Responsabilidade, sigilo e/ou não divulgação.

b) INTERNA (#INTERNA): é uma informação do Economus que o Instituto não tem interesse em divulgar publicamente, sendo consideradas, usualmente, informações internas para a realização de nossas atividades em prol dos negócios da Entidade. Tais dados podem ser acessados sem restrições por todos os colaboradores, fornecedores e prestadores de serviços do Economus, mediante a vigência de contrato e assinatura de Termo de Responsabilidade, sigilo e/ou não divulgação.

c) PÚBLICA (#PÚBLICA): é uma informação do Economus que pode ser divulgada sem restrição, sendo seu caráter informativo, comercial ou promocional. É destinada ao público interno e externo ou ocorre devido ao cumprimento de legislação vigente.

1.5.9. Requeremos de todo o público abrangido por essa política o respeito aos seus preceitos, independentemente do local de realização de suas atividades, inclusive quando em regime de teletrabalho.

1.5.10. **Tratamento de Incidentes de Segurança e/ou de Dados Pessoais**

1.5.10.1. Definimos procedimentos formais para notificação de falhas e incidentes de segurança da informação e procedimentos de resposta a incidentes.

1.5.10.2. Relatamos por meio dos canais apropriados, o mais rapidamente possível, os incidentes, as vulnerabilidades ou ameaças à segurança da informação.

1.5.10.3. Dispomos de um Programa de Mitigação de Incidentes, o qual é guia específico para o tratamento, prevenção e procedimentos para eventuais incidentes de violação de dados pessoais.

1.5.11. **Gestão de Ativos de Segurança da Informação**

1.5.11.1. Definimos ativos de segurança da informação como recursos corporativos que possuam valor para o Instituto e que devem ser protegidos. Listamos na sequência, de forma não conclusiva, itens que se enquadram nessa definição:

a) Hardware: computadores, servidores, impressoras, assim como dispositivos de comunicação e de armazenamento;

b) Software: quaisquer programas, sistemas operacionais, aplicativos e similares, sejam eles comprados (licenciados) ou gratuitos;

c) Informação: bases de dados, arquivos em diversos formatos eletrônicos (pdf, doc, xls, etc.), mas também documentos físicos e formulários;

d) Infraestrutura: acomodações, eletricidade e condicionamento de ar;

e) Pessoas: sejam eles empregados do Instituto, conselheiros, cedidos ou terceirizados;

f) Serviços terceirizados: serviços jurídicos, de tecnologia, de limpeza, e outros. Também inclui serviços online, como armazenamento ou sistemas em nuvem.

1.5.11.2. Inventariamos nossos ativos de segurança da informação, considerando sua condição de elementos-chave na identificação de riscos, ameaças e vulnerabilidades.

1.5.11.3. Definimos gestores aos ativos de segurança da informação. Todo item que compor o inventário de ativos de Segurança da Informação do Instituto deve obrigatoriamente conter a identificação de seu responsável primário na Entidade.

1.5.11.4. Priorizamos o uso de documentos digitais e incentivamos a digitalização do histórico de documentos físicos com vias ade promover uma gestão mais segura da informação e eticamente alinhada a princípios socioambientais.

1.5.12. **Gestão de Risco**

1.5.12.1. Identificamos os riscos inerentes à segurança da informação, às vulnerabilidades, às ameaças e os impactos nocivos que envolvam os processos de negócio e ativos de informação do Economus para que se busquem formas de mitigá-los.

1.5.13. **Gestão de Continuidade**

1.5.13.1. Avaliamos e corrigimos as vulnerabilidades, as ameaças, os riscos e os impactos que envolvem os ativos de informação do Economus, por meio da gestão de riscos de segurança e continuidade dos negócios, procedimentos de teste e de avaliação periódicos, em intervalos regulares.

1.5.14. **Auditoria e Conformidade**

1.5.14.1. Estruturamos controles que possibilitem a rastreabilidade dos acessos às informações do Economus e das atividades executadas pelos usuários.

1.5.14.2. Reservamo-nos ao direito de acessar quaisquer documentos, arquivos e informações que estejam armazenadas em nosso ambiente e de monitorar o tráfego de informações efetuado em nossas redes de comunicação, incluindo o acesso à internet e o uso do correio eletrônico corporativo.

1.5.14.3. Desautorizamos nossos usuários de realizarem testes com a finalidade de averiguar uma fragilidade suspeita relativa à Tecnologia da Informação do Economus.

1.5.14.4. Incentivamos, quando da detecção de fragilidades ou de suspeita de sua existência, que a situação seja comunicada à GEGOV/RISCO.

1.5.15. **Controle de Acesso**

1.5.15.1. Exigimos o uso de crachá de identificação do Economus, o qual apresenta uso obrigatório, pessoal e intransferível e deve ser mantido visível durante a permanência nas dependências do Instituto.

1.5.15.2. Realizamos o controle da entrada no Instituto, seja por meio de informação biométrica, crachá de identificação ou ainda, por meio de número de matrícula.

1.5.15.3. Responsabilizamos os usuários dos recursos de Comunicação e Tecnologia da Informação, os quais são identificados individualmente por uma chave e uma senha de acesso, pelo sigilo de sua senha e pelas atividades realizadas sob sua identificação.

1.5.16. **Uso de e-mail e Acesso à Internet**

1.5.16.1. Exigimos responsabilidade e boa-fé de nossos usuários na utilização dos recursos de Comunicação e de Tecnologia da Informação do Economus no sentido de que os utilizem somente para atividades lícitas, éticas, administrativamente admitidas e que estejam relacionadas ao seu trabalho.

1.5.17. **Lei Geral de Proteção de Dados**

1.5.17.1. Tratamos os dados dos titulares em linha com os requerimentos legais vigentes, sempre visando proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

1.5.17.2. Exigimos de parceiros de negócios, quando na posição de controlador, que atendam a todos os requerimentos legais e institucionais vigentes.

1.5.17.3. Agimos com o devido cuidado e zelo, quando na posição de operador, mesmo que o controlador dos dados não tenha realizado requerimentos específicos sob a égide da LGPD.

1.5.17.4. Desenvolvemos nossos sistemas, práticas e negócios sob um arcabouço institucional baseados em uma conduta ética, no atendimento aos requerimentos legais vigentes e em linha com os conceitos de privacidade e segurança desde a concepção.

1.6. Glossário

a) Acesso à informação – É o ato de estabelecer contato com a informação.

b) Ameaça – Causa potencial de um incidente indesejado, que pode resultar em dano para um ativo organizacional ou para a Entidade.

c) Armazenamento de informações – É a guarda ou custódia da informação em um meio eletrônico (mídia) e/ou ambiente físico.

d) Ativo – Qualquer coisa que tenha valor para Economus.

e) Ciclo de vida da Informação – Período de existência da informação que compreende os processos de geração (criação e aquisição), armazenamento, acesso e manuseio, distribuição e transporte, divulgação e descarte da informação.

f) Classificação da Informação – Grau de sigilo atribuído à informação com base na sua importância para o Economus.

g) Confidencialidade – Propriedade que objetiva restringir o acesso à informação apenas às pessoas autorizadas.

h) Controle de acesso – Prática que visa a gerenciar o acesso aos ambientes físicos (ex.: prédios, salas, etc.) e lógicos (ex.: sistemas, aplicações, etc.) de uma organização, tomando por base processos de identificação, autenticação, autorização e auditoria. Esses processos são validados por pessoas (guardas, recepcionistas, etc.), dispositivos biológicos, mecânicos ou tecnológicos, muitas vezes utilizados de forma integrada.

i) Custodiante da Informação – Aquele que tem a guarda da informação.

j) Dado – Qualquer elemento identificado em sua forma bruta que, em determinado contexto não conduz, por si só, à compreensão de determinado fato ou situação.

k) Disponibilidade – Propriedade que objetiva manter a informação acessível a quem dela precisa de forma tempestiva, relevante e suficiente.

l) Distribuição da informação – É o transporte ou transmissão da informação por múltiplos canais de comunicação.

m) Divulgação da informação – É a comunicação da informação almejando atingir o maior número possível de pessoas dentro de um público-alvo preestabelecido.

n) Gestor da informação – É o dono da informação, responsável por classificá-la e rotulá-la, bem como controlar o acesso a essa informação.

o) Gestão da Segurança de Informação – abrange a criação de processos voltados ao monitoramento contínuo da integridade das informações, à prevenção de ataques, ao furto de dados e acesso inadequado às informações, assegurando em casos emergenciais, o pronto restabelecimento dos sistemas e o acesso seguro às informações.

p) Incidente de Segurança da Informação – Evento com impacto negativo que possa comprometer a confidencialidade, integridade ou disponibilidade da informação.

q) Informação – conjunto de dados devidamente ordenados de forma a promover significado a algo e ser útil tornando-se assim em um recurso crítico para a definição da estratégia de uma organização, devendo, assim, ser tratada como um ativo do Instituto.

r) Informações não públicas – São as informações classificadas como confidenciais ou internas.

s) Integridade – Propriedade relativa à manutenção da informação protegida de possíveis modificações não autorizadas, imprevistas ou não intencionais, bem como protegidos os seus métodos de processamento.

t) Responsabilidade – Obrigações e deveres da pessoa que ocupa determinada função em relação ao acervo de informações.

u) Rotulagem – Registro do nível de classificação atribuído a uma informação.

v) Segurança da Informação – visa garantir que somente usuários autorizados (confidencialidade) possuem acesso à informação completa e precisa (integridade), quando esta for necessária (disponibilidade).

w) Sistemas Informatizados – Incluem a rede de computadores, as bases de dados, os programas de computador ou qualquer outro sistema capaz de armazenar ou transmitir dados eletronicamente, tais como correio eletrônico, e-mail, redes de automação de escritório, intranet, internet, etc.

x) Usuário – Aquele que utiliza os Recursos de Comunicação e de Tecnologia da Informação para realizar as suas atividades de trabalho no Economus.

y) Vulnerabilidade – Fragilidade decorrente da insuficiência de tratamento ou controle, que pode ser explorada por uma ou mais ameaças.

z) Titular – Pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.

aa) Controlador – Pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais. É um agente de tratamento.

bb) Operador – Pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador. Também é um agente de tratamento.

1.7. Referências Legais e Normativas

1.7.1. ABNT NBR 16167:2020 - Segurança da informação - Diretrizes para classificação, rotulação, tratamento e gestão da informação.

1.7.2. ABNT NBR ISO/IEC 27014:2021 - Segurança da informação, segurança cibernética e proteção da privacidade - Governança da segurança da informação.

1.7.3. ABNT NBR ISO/IEC 27005:2019 - Tecnologia da informação — Técnicas de segurança — Gestão de riscos de segurança da informação.

1.7.4. ABNT NBR ISO/IEC 27004:2017 - Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Monitoramento, medição, análise e avaliação.

1.7.5. ABNT NBR ISO/IEC 27032:2015 - Tecnologia da Informação - Técnicas de segurança - Diretrizes para segurança cibernética.

1.8. Histórico de Atualização

1.8.1. Essa política será revisada a cada 2 (dois) anos, ou em prazo inferior, seja por compliance regulatório ou por decisão estratégica.

Versão	Data	Nota Técnica	Descrição das Alterações	Próxima atualização
01	10/08/2018	2018/119	Criação do documento	até 10/08/2020
02	30/07/2020	2020/066	Revisão e atualização	até 30/07/2022
03	22/09/2022	2022/077	Revisão e atualização	Até 22/09/2024