| | |
|---|---|
| **TÍTULO:** | Política de Segurança da Informação - PSI |
| **CLASSIFICAÇÃO:** | Documento Executivo |
| **REFERENCIAL NORMATIVO** | Resolução CGPC nº 13, de 1º de outubro de 2004<br>Lei nº 13709, de 14 de agosto de 2018 |
| **ASSUNTO:** | Estabelecer as diretrizes, os princípios e os requisitos para Gestão Estratégica da Segurança da Informação e da Proteção da Privacidade na REGIUS. |
| **ELABORADOR:** | Área de Tecnologia |
| **APROVAÇÃO:** | **REVISÃO 00**<br>Aprovada na 598ª reunião do Conselho Deliberativo, de 27/07/2021. |

**INDICE**

## 1. INTRODUÇÃO

A presente política vem estabelecer as diretrizes para Gestão Estratégica da Segurança da Informação na REGIUS, referenciadas nos princípios basilares do sistema de gestão de segurança da informação, de forma que os requisitos de segurança preservem a confidencialidade, integridade e disponibilidade da informação, por meio de processo de gestão de riscos capaz de fornecer a confiança para as partes interessadas, de modo que os riscos sejam adequadamente gerenciados e que a segurança da informação esteja no centro do desenvolvimentos de projetos, processos ou produtos oferecidos pela REGIUS. E, ainda que os normativos e os planos que suportam o sistema de segurança, dentre outras finalidades, visem instituir e implementar os controles de segurança da informação, observando-se a estratégia do negócio, as regulamentações, legislação e contratos e os requisitos para se estabelecer um ambiente livre de ameaças, de modo a preservar dados e informações, considerando a segurança física, técnica e organizacional.

## 2. OBJETIVO

Estabelecer os princípios, diretrizes e as posturas que orientarão a gestão segurança da informação, visando preservar os pilares da confidencialidade, a integridade e a disponibilidade das informações na gestão da REGIUS, considerando os aspectos físicos, lógicos e comportamentais.

De forma que o Sistema de Gestão de Segurança da Informação da REGIUS seja capaz de preservar a segurança e privacidade dos dados e informações das partes que se relacionam com a entidade, de sustentar o propósito da REGIUS no cumprimento do seu referencial estratégico, de demonstrar o respeito ao contrato previdenciário e seu dever de fidúcia com participantes, assistidos, patrocinadores, instituidores, garantindo, assim, a preservação da Entidade e dos planos de benefícios, a construção de relações duradoras e a demonstração da credibilidade e prestígio no mercado previdenciário.

## 3. CONCEITOS E DEFINIÇÕES

**Dado:** é um fato ou uma série de fatos correlacionados ou não.

**Informação:** é o dado que tem significado para quem o recebe, podendo estar ou não relacionado a outros dados, portanto, trata-se de ativo intangível.

**Ativo:** é o que tem valor para o proprietário, seja indivíduo ou organização.

**Tipos de informação:** é forma que a informação é apresentada, podendo ser impressa ou escrita em papel; Verbal (conversas ou apresentações); Apresentada (filmes/fotos); armazenada eletronicamente (discos, bancos de dados); transmitida pelo correio ou por meios eletrônicos.

**Ciclo de vida da informação:** é conjunto de etapas do caminho da informação e compreende a criação, o armazenamento, a utilização, o compartilhamento, o uso, o arquivamento e a destruição.

**Informática:** é o processo usado para converter dado em informação.

**Segurança da Informação:** é conjunto de mecanismos, padrões, regras, normas e diretrizes que irão garantir a proteção das informações corporativas contra ameaças, com a finalidade de garantir a continuidade do negócio, sem prejudicar a operação, minimizando os riscos de perdas ou violação de informações, que possa prejudicar o negócio e os clientes.

**Elementos do sistema de informação:** sãos as regras, os meios, os procedimentos e as pessoas.

**Sistema de informação:** é o fluxo da informação que envolve o processamento, armazenamento, transferência de acordo com a forma que a informação de se apresenta e o seu regramento.

**Tecnologia da Informação:** é mecanismo de suporte ao sistema de informação e tem a função de coletar, processar, armazenar e transferir informações.

**Acesso remoto:** é uma tecnologia que permite a conexão à distância, feita com segurança de dados em ambos os lados, em que um computador consegue acessar um servidor/computador privado – normalmente de uma empresa – que não está fisicamente conectado à rede, por exemplo: VPN - Virtual Private Network (Rede Privada Virtual), Teamviewer.

**Ataque cibernético/ciberataque:** é a ação praticada por hackers que consiste na transmissão de vírus (arquivos maliciosos) que infectam, danificam e roubam informações de computadores e demais bancos de dados online, por exemplo;

**Arquivo digital:** é um documento eletrônico caracterizado pela codificação em dígitos binários e acessado por meio de sistema computacional. Todo documento digital é eletrônico, mas nem todo documento eletrônico é digital (transformado do papel para digital). Exemplos: texto em PDF, planilha de cálculo em Excel, áudio em MP3, filme em AVI.

**Ativos de informação:** é qualquer componente que sustenta um ou mais processos de negócio de uma unidade ou área que a segurança da informação visa proteger tais como: base de dados, contratos e acordos, documentação de sistema ou de negócios, infraestrutura de tecnologia, manuais, material de treinamento, procedimentos, planos de continuidade de negócio.

**O valor da informação:** é a referência de importância da informação para o negócio e, é balizador de sua classificação e refletida nos controles e requisitos de segurança para o negócio.

**Dados pessoais sensíveis:** São dados que estejam relacionados a características da personalidade do indivíduo e suas escolhas pessoais, tais como origem racial ou ética, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente a saúde ou vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

**Dados pessoais:** é toda informação relacionada a uma pessoa identificada ou identificável, não se limitando, portanto, a nome, sobrenome, apelido, idade, endereço residencial ou eletrônico, podendo incluir dados de localização, placas de automóvel, perfis de compra, número do Internet Protocol (IP), dados acadêmicos, histórico de compras, entre outros. Sempre relacionados a pessoa viva.

**GED – Gerenciamento Eletrônico de Documentos:** é ferramenta (sistema) de organização, transmissão e guarda de documento podendo esses documentos serem eletrônicos ou digitais.

**Incidente de Segurança:** é qualquer evento adverso, confirmado ou sob suspeita, relacionado a sistemas ou a própria informação, levando a perda de um ou mais princípios básicos de Segurança da Informação: confidencialidade, integridade e disponibilidade. Um grande incidente que ameaça a continuidade do negócio é chamado de desastre.

**Terceiros:** é o relacionamento contratual com empresas especializadas que objetiva a transferência planejada de atividades secundárias.

**VPN:** Virtual Private Network – é Acesso à rede corporativa por meio de uma rede doméstica.

**WiFi:** Wireless Fidelity – é a rede sem fio para acesso à Internet.

**Vulnerabilidade:** – Fraqueza de um ativo ou controle que pode ser explorado por uma ou mais ameaças, por exemplo: desktop sem proteção de senha, portas abertas no firewall, antivírus desatualizado, baixo nível de segurança física que permite qualquer um entrar na sala dos servidores etc.

**Risco:** É a probabilidade de um agente de ameaça tirar proveito de uma vulnerabilidade e isso gerar impacto no negócio (risco=ameaça+vulnerabilidae+probabilidade+potencial impacto).

## 4. PRINCÍPIOS

- Confiança
- Legalidade
- Respeito

## 5. PILARES DA SEGURANÇA DA INFORMAÇÃO

Os aspectos da Confiabilidade, atributos do princípio da confiança, representam o tripé da segurança da informação: confidencialidade, integridade e disponibilidade (CID), cujas medidas de proteção serão estabelecidas no Manual de Segurança da Regius.

**Confidencialidade:** a informação não disponibilizada ou divulgada a indivíduos, entidades ou processos não autorizados. A confidencialidade possui ainda, a característica de **exclusividade** que é a condição em que apenas usuários autorizados tenham permissão para acessar a informação e de **privacidade** que consiste em limitar o acesso às informações pessoais;

**Integridade:** é a propriedade da exatidão e completeza da informação. Reúne as características de serem exatas, integras, completas, válidas e de possível verificação. Daí a condição de que apenas alterações autorizadas podem ser realizadas para não comprometer a exatidão da informação.

Podem ser consideradas como característica da integridade: a **Autenticidade** e **o Não Repúdio**. A autenticidade é a garantia de que a informação é proveniente de fonte autêntica, ou seja, se refere à manutenção das condições iniciais, da mesma forma que foram produzidas e armazenadas e, que não foi alvo de mutação ao longo de um processo. O **Não Repúdio** refere-se à impossibilidade de negar a autoria em relação a uma transação feita.

**Disponibilidade:** condição em que a informação deve ser disponível para usuários autorizados quando solicitado. É a condição de ser acessível e utilizável sob demanda e autorização. A disponibilidade congrega, ainda, as características de **prontidão, continuidade e robustez,** onde sistemas precisam estar disponíveis quando necessários, precisam suportar a continuidade do negócio e as atividades diárias em uma falha e, precisam ter capacidade suficiente para suportar as atividades necessárias ao negócio.

## 6. ABRANGÊNCIA

Esta Política deverá ser observada por todos os integrantes e colaboradores da entidade incluindo as partes relacionadas e, deverá ser aplicada a todos os sistemas de informações e processos coorporativos da REGIUS, de forma que seja garantida a segurança das informações e dos recursos computacionais.

## 7. DIRETRIZES FUNDAMENTAIS

I. Deverá ser implementado um conjunto adequado de controles, incluindo: Politicas, processos, procedimentos, estrutura organizacional, funções de software e hardware;

II. O arcabouço estrutural e normativo deverá prevenir a perda de dados, assegurar a privacidade, proteger a propriedade intelectual da entidade, minimizar perdas, garantir a continuidade do negócio;

III. Todos os dados e informações produzidas para e pela REGIUS, totais ou parciais, físicas ou lógicas, são de propriedade da REGIUS, assim como os equipamentos fornecidos para o armazenamento, acesso e o controle;

IV. Todos os recursos baseados em Tecnologia da Informação ou produzidos por estes, estão sujeitos ao monitoramento e rastreabilidade, possibilitando a pronta resposta a incidentes de segurança;

V. A REGIUS, como responsável pelos dados e informações de participantes, assistidos, beneficiários, ex-participantes, patrocinadoras, instituidoras, entes federativos e parceiros, os declara sigilosos, logo devem ser tratados assim pelos seus empregados e terceiros, usando como parâmetro a Lei Nº 13.709/ 2018, Lei Geral de Proteção de Dados, bem como normativos internos relacionados com o tema.

VI. O acesso de empregados e terceiros aos ambientes lógicos e físicos é restrito e controlado. O acesso inicial considerará o princípio do menor privilégio, que estabelece os recursos mínimos de trabalho, podendo ser alterado conforme as atividades definidas pelo processo, alçada, cargo ou função;

VII. Os dados e informações, independente do seu formato, devem ser classificados quanto a sua confidencialidade, conforme sua importância estratégica para a Entidade. A classificação definirá a forma como as informações serão: armazenadas, copiadas, transmitidas, manuseadas, descartadas ou destruídas. As informações ainda serão classificadas quanto ao grau de sigilo.

VIII. Esta Política e as normas internas relacionadas devem integrar os contratos e acordos comerciais, definindo claramente os papéis, responsabilidades e os acordos de confidencialidade das partes envolvidas, quanto aos níveis de processamento de dados e informações, segurança, monitoramento e requisitos de contingência;

IX. Os empregados e terceiros devem utilizar os recursos e informações, seguindo os princípios do Código de Conduta e Ética e o Manual de Segurança da REGIUS, sem afetar ou causar prejuízo a outrem;

X. Todas as espécies de pressões e chantagens devem ser denunciadas;

XI. No tocante às informações sob responsabilidade da REGIUS, é vedado o manuseio sem estar expressamente previsto em normativos internos ou aprovação do gestor responsável;

XII. Todo e qualquer programa ou aplicativo a serem utilizados pela REGIUS deverão ser previamente aprovados pela Diretoria Executiva que observará a garantia da segurança das informações dos participantes, assistidos e beneficiários bem como avaliará a exposição aos riscos corporativos;

XIII. Os empregados e terceiros devem seguir as diretrizes de segurança quanto ao uso de Drives Virtuais, Mídias Removíveis e da porta USB;

XIV. Todos os acessos à Internet serão monitorados e registrados, podendo ser negados nos sites de conteúdo inadequado e/ou que tragam risco à segurança de TIC;

XV. As regras e diretrizes de segurança são interpretadas de forma que todas as suas determinações são obrigatórias sem exceções;

XVI. Todos os colaboradores são responsáveis pela segurança da informação.

## 8. RESPONSABILIDADES

**8.1.** Conselho Deliberativo – apreciar as proposições e deliberar a respeitos das Diretrizes (linhas mestras) para a garantir a segurança das informações e dos recursos computacionais.

**8.2.** Diretoria Executiva – submeter as diretrizes (linhas mestras) ao conselho deliberativo, promover a gestão estratégica do sistema de gerenciamento de segurança da informação e desenvolver a estratégia de segurança geral.

**8.3.** Conselho Fiscal - promover a análise crítica do sistema de segurança da informação e propor medidas físicas, técnicas e organizacionais que possam ser implementadas para o garantir ou aumentar a segurança das informações e dos recursos computacionais.

**8.4.** COMED - conduzir o procedimento administrativo disciplinar por infração ou violação às diretrizes institucionais expressas em Políticas, Códigos de Conduta e Ética e legislação vigente.

**8.5.** Diretoria responsável pela gestão de riscos e controles – promover o gerenciamento dos riscos e a fiscalização da Segurança da Informação.

**8.6.** Diretoria responsável pela Segurança Informação - conduzir o regramento da segurança da informação na entidade e prover as condições de implementação das regras.

**8.7.** Gerência responsável pela Segurança da Informação - garantir a observância à PSI e promover a implementação dos requisitos, normas e regras necessárias ao direcionamento dado à segurança da informação, tais como:

- Zelar para que sejam mantidos plano de recuperação de desastres (PRD) e o plano de continuidade de negócios (PCN), atualizados e aplicáveis;

- Manter atualizados os códigos de condutas e as regras que versam sobre trabalho remoto, gestão de ativos, tratamento de mídias, regras de BYOD (bring your own device);

- Propor a execução de pentest;

- Orientar o gerenciamento de incidentes de segurança da informação;

- Supervisionar a aplicação das medidas físicas, técnicas e organizacionais pelas coordenações subordinadas;

- Estabelecer o padrão adequado com relação a qualidade dos sistemas computacionais.

- Propor plano treinamento de segurança da informação,

**8.8.** Da Unidade Organizacional responsável pela coordenação de tecnologia da informação

- Zelar, em nível físico e lógico, pelos ativos de informações e de processamento de dados no âmbito da REGIUS;
- Identificar as vulnerabilidades que podem ser exploradas por agentes internos ou externos e adotar medidas de forma a prevenir o dano ou desastre;
- Aplicar as medidas de segurança físicas, técnicas e organizacionais;
- Monitorar e reportar à Diretoria Executiva qualquer uso inadequado de dados, informações ou condutas que possam ferir esta Política ou normas internas relacionadas;
- Estabelecer supervisão constante das tentativas de violação da segurança da informação;
- Manter atualizadas normas e os procedimentos que visam:

✓ Controle de acesso, classificação e tratamento da informação, segurança física e do ambiente;

✓ Orientação aos usuários finais como: Uso aceitável de ativos, Mesa Limpa e tela limpa, transferência de informações, dispositivos móveis e trabalho remoto, restrições sobre o uso e instalação de software;

✓ Backup, transferência de informação, proteção contra código maliciosos.

- Coordenar a aplicação das medidas para identificar e tratar vulnerabilidade técnicas, controles criptográficos, segurança nas comunicações, proteção e privacidade da informação de identificação pessoal, relacionamento na cadeia de suprimento.

**8.9.** Dos Colaboradores e Terceiros.

- Preservar a integridade e guardar sigilo das informações que fazem uso, bem como zelar e proteger os respectivos recursos usados para produzir, acessar ou armazenar os dados e informações;

- Cumprir e disseminar os princípios desta Política, sob pena de incorrer em sanções disciplinares previstas nas normas internas e legislação vigente;
- Utilizar recursos, dados e informações da Regius somente para fins coorporativos;
- Responder pelo uso de recursos e informações, bem como seus efeitos;
- Comunicar, por escrito, aos órgãos que regem esta Política o conhecimento de qualquer irregularidade ou desvio.

## 9. TEMPORALIDADE

| Responsável pela publicação | Temporalidade | Arquivo digital |
|---|---|---|
| GEGOL | Até 3 anos, com avaliação mínima, a cada ano.. | CloudDocs |

## 10.VIOLAÇÕES E PENALIDADES

As sanções serão as previstas no Regulamento Disciplinar, Código de Conduta e Ética e legislação vigente.

## 11. CONSIDERAÇÕES FINAIS

A implementação das diretrizes tratadas nesta Política será feita por outros instrumentos normativos, conforme o direcionamento do sistema normativo da Entidade.

Esta Política deve ser atualizada e avaliada na periodicidade que a mantenha atualizada ao direcionamento, entrando em vigor a partir da sua aprovação pelo Conselho Deliberativo REGIUS.

As alterações e os casos omissos na presente Política serão tratados pela Diretoria Executiva.