Agros
Instituto UFV de Seguridade Social

ANS - nº 368920

RESOLUÇÃO CDE Nº 459/2022

Aprova a revisão da Política de Segurança da Informação do Agros – Instituto UFV de Seguridade Social

O Conselho Deliberativo do Agros – Instituto UFV de Seguridade Social, no uso de suas atribuições, considerando o disposto no processo administrativo Agros nº 028/2021,

RESOLVE:

Art. 1º Revogar a Resolução CDE nº 259/2011, que é por esta substituída.

Art. 2º Aprovar a Política de Segurança da Informação do Agros – Instituto UFV de Seguridade Social, revisada, conforme documento anexo.

Viçosa, 23 de agosto de 2022.

José Júlio de Souza

Eduardo Rezende Pereira

Augusto César de Queiroz

Moacir Albuquerque Gomes de Lima

Luciana Aparecida Silva

Vicentina das Dores Martins Ferreira

Adriel Rodrigues de Oliveira

Jansen Cardoso Pereira

Moacil Alves de Souza

Política de Segurança da Informação

Viçosa, agosto de 2022

Agros – Instituto UFV de Seguridade Social
Av. Purdue, s/n Campus da UFV Viçosa-MG 36570-900
Fone: (31) 3899-6550

Sumário

1. Introdução

A informação é cada vez mais um bem valioso para as pessoas, empresas e governos. Após sua geração, pode circular em diversos meios de comunicação e sua divulgação descontextualizada ou desautorizada pode gerar graves consequências, portanto, deve ser tratada com muito cuidado e rigor. De uma forma crescente, as organizações estão diante de constantes ameaças relacionadas às informações com que lidam e que, se concretizadas, podem resultar em grandes prejuízos para seus negócios e/ou seus públicos.

Diante desse cenário, a gestão da segurança da informação tornou-se necessária em todas as empresas. Sendo assim, a política ora apresentada torna-se um documento de grande importância para nortear o gerenciamento da segurança da informação no Agros, alinhando-se à política institucional da empresa.

A expressão “segurança da informação” pode ser entendida como uma área do conhecimento que salvaguarda os ativos da informação contra acessos indevidos, modificações não autorizadas e até mesmo contra sua indisponibilidade. Ela não está restrita somente a sistemas computacionais, informações eletrônicas ou sistemas de armazenamento, o conceito se aplica a todos os aspectos de proteção de informações e dados em diferentes suportes, de diferentes naturezas.

Reafirmando a importância da proteção da informação, a Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709 de 14/08/2018, estabeleceu normas para obtenção, utilização e armazenamento de dados pessoais no Brasil. A LGPD, em seu conceito geral, estabelece que qualquer informação relacionada a uma pessoa natural (chamada de titular) que possa gerar sua identificação deve receber tratamento especial, assegurando o direito à privacidade e à proteção de dados pessoais dos cidadãos, por meio de práticas transparentes e seguras, garantindo direitos e liberdades fundamentais. Em sua essência, a LGPD busca proteger a privacidade dos titulares de dados pessoais.

Segundo a ISO/IEC 17799:2005, são princípios básicos da segurança da informação os atributos de confidencialidade, integridade, disponibilidade e autenticidade, que podem ser assim definidos:

- ***Confidencialidade*** - propriedade que limita o acesso à informação somente às entidades legítimas, ou seja, aquelas autorizadas pelo proprietário da informação;
- ***Integridade*** - propriedade que garante que a informação manipulada mantenha todas as características originais estabelecidas pelo proprietário da informação, incluindo controle de mudanças e garantia do seu ciclo de vida (geração, manutenção e descarte);
- ***Disponibilidade*** - propriedade que garante que a informação esteja sempre disponível para o uso legítimo, ou seja, por aqueles usuários autorizados pelo proprietário da informação;
- ***Autenticidade*** - certeza de que um objeto (informação) provém das fontes anunciadas e que não foi alvo de mudanças ao longo de um processo. Na telecomunicação, uma mensagem será autêntica se for, de fato, recebida na íntegra, diretamente do emissor.

Para o Agros, que trabalha com informações críticas de seus participantes e beneficiários, quadro corporativo, patrocinadores, instituidores e prestadores de serviço, o tratamento seguro da informação é imprescindível para garantir o respeito a esses quatro princípios.

A Confidencialidade não se sobrepõe à transparência, em respeito ao que consta no Código de Ética do Instituto. O princípio da Confidencialidade se aplicará naqueles casos em que ficar demonstrada a necessidade da proteção de informações comprovadamente sensíveis, sejam elas dados estratégicos ou informações pessoais protegidas em lei. Também nesta Política, vale o princípio geral que a transparência é regra, e o sigilo, a exceção.

Quando se fala em segurança da informação, deve-se ter em mente também que o alicerce que assegura os atributos da informação de qualidade é formado por três pilares:

- **Físicos -** acessos físicos, cabeamentos, climatizadores, nobreaks, extintores de incêndio, armazenamento de backup, vigilância, etc.;
- **Tecnológicos -** antivírus, firewall, criptografia, acessos a rede e sistemas, qualidade dos sistemas, etc.;
- **Humanos -** conscientização, informação, capacitação, termo de responsabilidade e confidencialidade, defensiva quanto à engenharia social, etc.

Ao se tratar dos aspectos humanos de segurança da informação, não se pode deixar de mencionar a “Engenharia Social”, uma vez que é comum que ameaças resultam da ação de pessoas que utilizam tal técnica. A Engenharia social, segundo Peixoto (2006), é:

> “a ciência que estuda como o conhecimento do comportamento humano pode ser utilizado para induzir uma pessoa a atuar segundo o seu desejo. Não se trata de hipnose ou controle da mente, as técnicas de Engenharia Social são amplamente utilizadas por detetives (para obter informação) e magistrados (para comprovar se um declarante fala a verdade). Também é utilizada para lograr todo tipo de fraudes, inclusive invasão de sistemas eletrônicos.”

2. Objetivos

2.1. Objetivo Geral

A Política de Segurança da Informação do Agros visa estabelecer diretrizes a serem seguidas para garantir a proteção das informações de sua propriedade e/ou sob sua guarda, considerando os quesitos de confidencialidade, integridade, disponibilidade e autenticidade, primando pelo cumprimento da missão: “*Gerir planos de previdência e de saúde com eficiência, segurança e sustentabilidade, proporcionando aos beneficiários condições para melhor qualidade de vida*.”

As diretrizes definidas nesta política direcionarão a construção e adoção de procedimentos e mecanismos que propiciem a segurança da informação no âmbito do Instituto.

2.2. Objetivos Específicos

Garantir a segurança da informação no exercício das atividades do Instituto, com base em normas e procedimentos a serem criados e adotados que colaborem com a construção de uma cultura corporativa em prol da segurança da informação. Para tanto, o Agros estabelece como questões a serem desenvolvidas nesta política:

i. Tratamento e classificação das informações;
ii. Procedimentos para os acessos físicos externos e internos do quadro corporativo e de terceiros;
iii. Acesso e uso da rede local, intranet e internet;
iv. Uso, instalação e qualidade dos softwares;
v. Uso de e-mail e outras aplicações de comunicação;
vi. Gestão de senhas de sistemas;
vii. Backup/restore;
viii. Atualização e utilização de softwares de proteção de dados (antivírus, firewall, antimalware etc.);
ix. Disponibilização de informações para terceiros (auditores, consultores, etc);
x. Relacionamento com os fornecedores de produtos e prestadores de serviços;
xi. Conscientização/treinamento do quadro corporativo para acesso e uso da informação;
xii. Definição de procedimentos para a recuperação de eventuais danos causados por incidentes ocorridos pela má utilização da informação e/ou indisponibilidade da informação, em Plano de Contingência Operacional.

2.3. Estrutura Normativa da Política de Segurança da Informação

A estrutura da política de Segurança da informação do Agros é composta por um conjunto de documentos hierarquicamente descritos a seguir, que devem passar por revisões periódicas e posterior aprovação da Diretoria Executiva (DEX) e Conselho Deliberativo (CDE):

- Política de Segurança da Informação → constituída por este documento, define a estrutura, as diretrizes e as obrigações referentes à segurança da informação.

- Normas de Segurança da Informação → descrevem todas as regras de segurança definidas de acordo com as diretrizes da Política, a serem seguidas em diversas

situações em que as informações são tratadas. Este documento deve ser aprovado pela Diretoria Executiva.

- Procedimentos de Segurança da Informação → visam instrumentalizar o disposto nas Normas e na Política, a fim de que as unidades administrativas do Agros adequem seus processos a esses normativos.

3. Diretrizes

A Política de Segurança da Informação do Agros tem sua estrutura alicerçada nas legislações aplicáveis, no Estatuto, Regulamentos, Código de Ética e Conduta, Política Institucional, Planejamento Estratégico e nas demais normas e documentos que abordem a questão. Ela orienta para a importância dos seguintes itens:

i. Obrigações e direitos de acesso, uso e manipulação da informação;
ii. Procedimentos operacionais de acesso, uso e manipulação da informação;
iii. Níveis e critérios adequados de proteção das informações que garantam a sua confidencialidade, integridade, disponibilidade e autenticidade, de acordo com a importância para a organização;
iv. Acessos a sistemas de gestão e controles internos, intranet e internet;
v. Instituição de Comitê Gestor da Segurança da Informação para acompanhamento da política, das normas e procedimentos;
vi. Criação do Termo de Conhecimento e Responsabilidade da Política de Segurança da Informação.
vii. Utilização das informações sob responsabilidade do Instituto apenas para as finalidades que foram coletadas.
viii. Orientação sobre acessos às instalações e informações restritas apenas a funcionários autorizados.
ix. Orientação para a elaboração dos contratos de prestação de serviço, de forma a cumprirem os padrões de segurança da informação estabelecidos nos documentos internos do Agros e na legislação vigente.

Destacam-se que os documentos preconizados nesta Política de Segurança da Informação do Agros, como Normas e Procedimentos, deverão ser:

i. Alinhados às estratégias do Agros;

ii. Simples e definidos de maneira clara e objetiva, em linguagem de fácil entendimento e totalmente alinhados à realidade do Instituto;
iii. Propícios à cultura corporativa de segurança da informação;
iv. Elaborados de forma a permitir a sua efetividade, envolvendo todos os colaboradores e os tornando corresponsáveis pela proteção da informação manuseada;
v. Flexíveis o suficiente para acompanhar a evolução da tecnologia e do negócio do Agros;
vi. Alinhados às boas práticas para a segurança da informação, respeitando os pilares da confidencialidade, disponibilidade, integridade e autenticidade;
vii. Aderentes ao Código de Ética e Conduta do Agros;
viii. Sujeitos a validações, de forma que se possa certificar que os processos operacionais definidos nos normativos estão sendo praticados da forma prevista, com consistência, regularidade e continuidade.

4. Responsabilidades

4.1. Geral

Funcionários, diretores, conselheiros, estagiários, jovens aprendizes, prestadores de serviço, terceirizados, auditores e consultores externos e qualquer outro órgão, setor ou pessoa que seja autorizado a acessar o ambiente tecnológico e/ou de informação do Agros têm o dever de:

i. Cumprir a Política de Segurança da Informação;
ii. Assinar termo de conhecimento e responsabilidade com a Política de Segurança da Informação;
iii. Buscar orientações com o superior hierárquico e/ou com o Comitê Gestor da Segurança da Informação, em caso de dúvidas e sugestões em relação à política, normas e/ou procedimentos de segurança da informação;
iv. Usar os recursos da Tecnologia da Informação (TI) do Agros exclusivamente para fins e interesses do Instituto, preservando a integridade dos equipamentos e da informação;
v. Estar consciente da classificação quanto a confidencialidade e importância da informação manuseada;

vi. Proteger as informações contra acesso, modificação, destruição ou divulgação não autorizados;
vii. Usar adequadamente, conforme os normativos internos, a rede local de computadores, intranet e internet;
viii. Comunicar ao Comitê Gestor de Segurança da Informação qualquer atitude que coloque em risco a segurança da informação no Agros.

4.2. Conselho Deliberativo (CDE)

i. Aprovar a Política de Segurança da Informação do Agros.
ii. Zelar pela Política de Segurança da Informação, apreciando relatório anual emitido pelos responsáveis por ela.
iii. Aplicar as sanções após a finalização do respectivo processo administrativo.
iv. Deliberar sobre os casos omissos.

4.3. Conselho Fiscal (CFI)

i. Fiscalizar o cumprimento da Política de Segurança da Informação do Agros;

4.4. Diretoria Executiva (DEX)

i. Nomear o Comitê Gestor da Segurança da Informação do Agros;
ii. Propor e encaminhar a Política de Segurança da Informação para o CDE;
iii. Acompanhar o monitoramento da Política de Segurança da Informação;
iv. Encaminhar ao Comitê de Ética as violações da Política de Segurança da Informação, para avaliação;
v. Acompanhar e autorizar ações de redução de incidentes que envolvam a segurança da informação no Agros, tais como catástrofes, intepéries, sinistros, bem como as rotinas que visem a recuperação de eventuais valores perdidos em função destes incidentes;
vi. Analisar as proposições feitas pelo Comitê de Ética e Comitê Gestor da Segurança da Informação, tomando as ações necessárias decorrentes dos encaminhamentos recebidos.

vii. Propiciar condições para o cumprimento desta Política.

4.5. Comitê de Ética

Em acordo com as situações previstas no Código de Ética e Conduta, caberá ao Comitê de Ética:

i. Apurar irregularidades que forem encaminhadas ao Comitê de Ética;
ii. Propor o enquadramento nas sanções aplicáveis nos casos de descumprimento da Política de Segurança da Informação;
iii. Sugerir medidas a serem tomadas para adequação à Política e Normas de Segurança da Informação ao Comitê Gestor de Segurança da Informação;
iv. Reportar ao Comitê Gestor de Segurança da Informação o desfecho de Processo Administrativo Disciplinar.

4.6. Comitê Gestor de Segurança da Informação

i. Estabelecer o Regimento Interno do Comitê Gestor de Segurança da Informação;
ii. Instituir o Termo de Conhecimento e Responsabilidade com a Política de Segurança da Informação;
iii. Acompanhar e elaborar normas e procedimentos de segurança da informação, juntamente com os gestores do Agros;
iv. Propor mudanças ou adequações na Política de Segurança da Informação;
v. Classificar, juntamente com os gestores do Agros, as informações quanto à disponibilidade, confidencialidade e integridade;
vi. Encaminhar à DEX as violações da Política de Segurança da Informação;
vii. Receber os Processos Administrativos Disciplinares do Comitê de Ética e tomar as providências cabíveis, conforme suas responsabilidades;
viii. Monitorar, controlar e revisar a Política de Segurança da Informação do Agros;
ix. Avaliar os incidentes de segurança e propor ações corretivas.

4.7. Gerentes e Assessores

i. Definir acessos de seus colaboradores aos módulos do sistema de gestão do Agros, intranet/internet, redes sociais e rede local de computadores em caso de

contratações, alterações de funções e desligamentos, fazendo a solicitação das atualizações nos sistemas para a GTI.

ii. Auxiliar o Comitê Gestor de Segurança da Informação na classificação das informações quanto à disponibilidade, confidencialidade e integridade;

iii. Auxiliar o Comitê Gestor de Segurança da Informação na elaboração de normas e procedimentos de segurança da informação.

4.8. Gerência de Tecnologia da Informação (GTI)

i. Auxiliar o Comitê Gestor da Segurança da Informação na classificação das informações quanto à disponibilidade, confidencialidade e integridade;

ii. Implementar procedimentos tecnológicos que possibilitem maior segurança da informação;

iii. Auxiliar o Comitê Gestor da Segurança da Informação na criação das normas e procedimentos de segurança da informação;

iv. Realizar treinamentos sobre os procedimentos técnicos relacionados à Tecnologia da Informação, necessários para cumprimento das normas de segurança da informação;

v. Aplicar os níveis de acessos a sistemas administrativos, intranet/internet e rede local, conforme definido pelas unidades administrativas, bem como finalizar ou alterar o acesso, conforme informações repassadas pela unidade administrativa e pela Gestão de Pessoas (GPE), decorrente de fim de vínculo empregatício, mudança de função, vínculos de estágios e terceirizados.

4.9. Assessoria Jurídica (ASJ)

i. Analisar a legislação quanto às exigências de órgãos fiscalizadores e reguladores do Agros em relação à segurança da informação;

ii. Avaliar os instrumentos jurídicos, de modo que possibilite o cumprimento das normas de segurança da informação do Agros.

4.10. Assessoria de Comunicação (ASC)

i. Divulgar a Política de Segurança da Informação, em toda a sua abrangência, a quem de direito;

ii. Revisar e manter as Normas de Comunicação e efetuar a divulgação de documentos em conformidade com as Normas de Segurança da Informação.

4.11. Gerência de Gestão de Pessoas (GPE)

i. Informar aos novos colaboradores sobre a Política e as Normas de Segurança da Informação do Agros;
ii. Solicitar assinaturas do Termo de Conhecimento e Aceite da Política de Segurança da Informação do Agros;
iii. Comunicar à GTI e às unidades administrativas relacionadas as novas contratações, movimentações internas de colaboradores, os desligamentos e qualquer outras alterações quanto ao quadro corporativo, para atualização do controle de acessos e permissão de utilização dos sistemas de informação.

4.12. Gerência Administrativa (GAD)

i. Manter a estrutura física da sede e das unidades de atendimento, visando a proteção dos equipamentos e dados do Agros;
ii. Gerenciar descartes de documentos, mídias de armazenamento e rascunhos, de modo a garantir a segurança da informação, de acordo com normativo próprio;
iii. Controlar, de forma corresponsável com a GPE quando se tratar de colaboradores, os acessos às dependências do Agros, para que somente pessoas credenciadas tenham acesso às instalações internas.

4.13. Secretaria Executiva (SEC)

i. Orientar as áreas, mediante solicitação, sobre as melhores práticas visando a segurança da informação de arquivos físicos, microfilmados ou digitalizados do Agros.
ii. Elaborar a norma de gestão, temporalidade e descarte de documentos.

4.14. Assessoria de Planejamento, Orçamento e Riscos (APR)

i. Dar suporte às demais unidades administrativas no gerenciamento de riscos de processos que envolvam a segurança da informação;

ii. Sugerir alterações nos processos para que eles estejam adequados às normas e procedimentos da Política de Segurança da Informação;

iii. Verificar periodicamente se as atividades do Agros estão sendo realizadas em conformidade com as leis, padrões éticos, regimento, regulamento e com as definições desta Política.

4.15. Gerência de Relacionamento (GRE)

i. Efetuar a triagem, registrar e controlar o acesso de pessoas nas dependências da sede e nas unidades de atendimento externas nos horários de funcionamento do Instituto;

ii. Estabelecer processos que permitam o pronto arquivamento e a garantia da integridade dos documentos manuseados na gerência;

iii. Estabelecer procedimentos de identificação de beneficiários, de acordo com o canal de atendimento;

iv. Estabelecer o limite de acesso dos colaboradores a informações, processos e rotinas, objetivando a garantia da confidencialidade e do sigilo no relacionamento com os beneficiários e prestadores de serviços;

v. Estabelecer e autorizar a liberação de acesso às aplicações no sistema de gestão do cadastro de participantes e beneficiários do Instituto, sistema de telefonia e arquivos na rede interna específica da gerência;

vi. Estabelecer melhores práticas para guarda dos celulares corporativos e procedimentos para impedir o acesso às gravações em caso de roubo ou perda.

5. Do Descumprimento da Política

Os fatos que caracterizem o descumprimento da Política de Segurança da Informação deverão ser encaminhados pelas unidades administrativas ou pelos colaboradores do quadro corporativo à Diretoria Executiva, que deverá dar conhecimento ao Comitê Gestor da Segurança da Informação ou, conforme o caso, ao Comitê de Ética do Instituto, ou decidir sobre as ações a serem adotadas.

6. Disposições Gerais

i. Compete à DEX tomar as medidas necessárias para a implantação do Comitê Gestor de Segurança da Informação;

ii. A DEX promoverá a nomeação e instalação do Comitê Gestor de Segurança da Informação no prazo de 30 dias após a aprovação desta Política;

iii. O Comitê Gestor de Segurança da Informação terá 6 (seis) membros efetivos, observada a seguinte composição:

   a. Um representante da Diretoria Executiva, que será o presidente do Comitê;
   b. Um membro do Conselho Deliberativo;
   c. Um membro do Conselho Fiscal;
   d. O gestor de TI;
   e. A assessora de comunicação.

iv. Os membros integrantes do Comitê Gestor de Segurança da Informação terão mandato de 3 (três) anos, podendo ser reconduzidos, por ato da DEX, por mais 3 (três) anos;

v. O Comitê Gestor de Segurança da Informação terá 90 (noventa) dias, após a sua nomeação e instalação, para elaborar o seu Regimento Interno, que deverá ser aprovado pelo CDE;

vi. Esta Política de Segurança da Informação e os demais normativos que a acompanha deverão ser revistos pelo Comitê Gestor de Segurança da Informação anualmente, por ocasião do aniversário de aprovação destes documentos, ou a qualquer tempo, por necessidade operacional, devendo ser encaminhados às instâncias pertinentes para aprovação.

7. Referências Bibliográficas

i. Código de Ética e Conduta – Agros 2019;
ii. ISO/IEC 17799:2005;
iii. Lei Geral de Proteção de Dados Pessoais - LGPD – nº 13.709/18, de 14/08/2018;
iv. Manual de Governança Corporativa – Agros 2008;
v. Política de Segurança da Informação do Agros, aprovada pela Resolução CDE 259, Ano 2011;
vi. Relatório PFM – Relatório de Avalição de Riscos – Agros - 4º Ciclo 2018 – PFM Consultoria & Sistemas;
vii. Citação do autor Peixoto – Engenharia Social