# POLÍTICA DE TI DA COOPAZ

## 1. Objetivo

A presente Política de Tecnologia e Segurança da Informação ("**Política**") visa estabelecer e organizar a abordagem, metodologia e responsabilidade para preservar a confidencialidade, integridade e a disponibilidade das informações da Cooperativa de Economia e Crédito Mútuo dos Funcionários da AstraZeneca do Brasil ("**COOPAZ**"). Esta Política refere-se ainda à segurança da informação e seus padrões de segurança, procedimentos e diretrizes, estando em conformidade com as políticas e procedimentos da COOPAZ, bem como com as políticas e procedimentos globais e locais de TI e segurança da informação da AstraZeneca do Brasil Ltda. ("**ASTRAZENECA**"). Esta Política cobre:

- Princípios de Segurança da Informação.
- O gerenciamento apropriado dos riscos associados a este tipo de informação.
- Oferecer suporte aos padrões específicos de segurança da informação.
- Adequação ao disposto nesta Política.

## 2. Cobertura

Esta Política se aplica a todos os cooperados e responsáveis por funções administrativas da COOPAZ e a quaisquer terceiros responsáveis por qualquer atividade que esteja conectada com o sistema ou ciclo (desenvolvimento, entrega, suporte e remoção) de serviços de Tecnologia da Informação ou sistemas contratados pela COOPAZ.

Esta Política também deverá ser aplicada a quaisquer terceiros por intermédio de contratos.

## 3. Escopo

Esta Política se aplica aos arquivos e às informações da COOPAZ armazenados em meio eletrônico, bem como aos serviços de informática, computadores e dispositivos, (incluindo plataformas, softwares, Serviços de Infraestrutura, Sistemas e Serviços de Computação na Nuvem), incluindo estruturas digitais aplicadas e difusas, sistemas e aplicações de computação que suportem ou transmitam tais arquivos e informações.

Este documento reforça e deve ser interpretado conjuntamente com seguintes documentos globais e locais da ASTRAZENECA: ITSEC – *Information Technology Security Policy*; *Corporate Information Technology Usage; Information and Records Management Global Standard; ITSEC – Secure Information Management Standard; ITSEC – Access Management Standard; ITSEC -IT Network Design; Configuration and Hardening Standard; ITSEC – Secure Electronic Data Transfer Standard; ITSEC -End User Computing Device Security Standard; ITSEC – Vulnerability Management Standard; ITSEC – User ID & Password Configuration Standard; ITSEC – IT Software Design; Configuration and Hardening Standard; ITSEC – Data Sanitization Standard; ITSEC – Security in Contracts Standards; ITSEC - Monitoring & Logging Standard, Incident Management; Manage Exceptions & Deviations to IT Policies, Standards or Processes – SOP; IT Privacy by Design Standard; Information Technology Acquisition Standard; e IT Security Standard Operating Procedure..*

## 4. Padrões e Procedimentos

### 4.1. Princípios

1. Sistemas de TI deverão ser geridos e desenvolvidos em conformidade com os padrões de segurança da COOPAZ e da ASTRAZENECA durante todo seu ciclo de vida.

2. Informação é uma peça chave para a continuidade de operação da COOPAZ. A confidencialidade (informação acessível para pessoal autorizado), integridade (proteção contra mudanças acidentais ou não autorizadas) e disponibilidade (a informação poderá ser acessada conforme a necessidade) da informação eletrônica deverão ser asseguradas.

3. Os Padrões de Segurança da Tecnologia da Informação (ITSEC) devem estar alinhados com as estratégias comerciais e capacidade prática. A comunicação segura das informações eletrônicas da COOPAZ é ponto fundamental ao negócio. Controles de Segurança devem considerar o uso potencial de tecnologia em dispositivos existentes ou em desenvolvimento para acessar as informações eletrônicas, além dos sistemas utilizados para armazenar e tratar informações da COOPAZ.

4. Esta Política e os padrões a ela relacionados respaldam a proteção de informações eletrônicas da COOPAZ aonde quer que elas estejam armazenadas, podendo, no entanto, serem acessadas independentemente do método de armazenamento e transporte.

5. Os controles de segurança instalados nos ativos de informação devem ser proporcionais aos riscos que tais ativos possam trazer ao negócio da COOPAZ.

6. As atividades dos serviços de informação devem ser consistentes com a estratégia de segurança da Tecnologia da Informação da ASTRAZENECA e da COOPAZ.

### 4.2. Mitigação e Avaliação de Risco

1. Informações críticas ao negócio mantidas em meio eletrônico deverão conter protocolos claros e documentados em relação a classificação de segurança da informação e o valor da informação em risco. As informações críticas mantidas em meio eletrônico deverão ser vinculadas a um administrador que será responsável por avaliar e revisar sua classificação periodicamente.

2. Sistemas de informação que armazenam e processam dados (e informações) da COOPAZ deverão receber uma avaliação de risco e deverão ser apreciados de acordo com um critério de aceitação de risco. Requisitos do negócio, gestão de informações e capacidades técnicas deverão ser levados em consideração nesta avaliação.

3. A gestão de riscos de informações e sistemas deverá ser colocada em prática sempre que o ambiente de operações sofrer mudanças significativas (i.e., *drives* regulatórios, ameaças, vulnerabilidades, e requisitos de segurança).

4. Sistemas e seus componentes deverão ser objeto de avaliação constante para a redução de riscos causados pela exploração de vulnerabilidades/exposição (i.e., programas sem uso, protocolos não seguros, usuários ou grupos com controles de acesso não seguros). Apreciação de riscos mandatórios (controle preliminar) deverão ser definidos de acordo com padrões técnicos de softwares, hardwares e networks. A partir destes padrões técnicos, é mandatório que sejam

definidas especificações para os principais componentes de tecnologia (i.e. para todos os sistemas em operação, aplicações e servidores).

## 4.3. Organização de Segurança da Informação

1. A COOPAZ definiu, com clareza, as atribuições e responsabilidades para prestação de serviço de TI e Segurança da Informação.

2. Contratos que envolvam a segurança da Tecnologia da Informação deverão indicar um colaborador da ASTRAZENECA como gerente de segurança de Tecnologia da Informação para os serviços de segurança contratados. Este colaborador deverá certificar-se de que todos os controles de segurança incluídos em contrato de prestação de serviços por terceiros sejam implementados, estejam operantes, além de monitorados e mantidos em conformidade com o contrato.

3. Contratos com terceiros deverão garantir que a completa e efetiva segurança da Tecnologia da Informação seja aplicada a todas as áreas relevantes. Os serviços de segurança da Tecnologia da Informação prestados deverão proteger a COOPAZ, assegurando os princípios fundamentais de confidencialidade, integridade e disponibilidade dos sistemas que tratam, transmitam ou armazenem informações.

4. Será designado ao *Data Privacy Officer* a função de supervisionar a aplicação desta Política e de revisá-la anualmente

## 4.4. Segurança Física e Ambiental

1. Procedimentos de segurança da informação para criação, ajuste, ou remoção de instalações, rede ou sistema/chave de acesso deverão estar à disposição do colaborador, contratante ou contratado e outros terceiros vinculados por contrato de trabalho. Os procedimentos deverão incluir considerações a respeito de equipamentos de uso pessoal ou de uso remoto (i.e. laboratórios e processos de controle) e a devolução de ativos de tecnologia emitidos pela COOPAZ e pela ASTRAZENECA incluindo, mas não se limitando a, dispositivos, tokens, PCs, tablets, iPads, telefones celulares e mídias removíveis.

2. Os padrões para as instalações de Segurança da Informação que

abrigam ou processam informações eletrônicas da COOPAZ serão auditados pela segurança funcional de Tecnologia da Informação.

3. As instalações, data centers, e outros centros dedicados a abrigar infraestrutura de TI que tratem informações eletrônicas da COOPAZ, deverão estar localizados em áreas controladas, protegidas por todo seu perímetro com barreiras físicas apropriadas, controle de acesso e ambiente. As instalações deverão ser fisicamente protegidas de acesso não autorizado, dano ou interferência e manutenção do controle de acesso ao perímetro. A proteção fornecida deverá observar os riscos identificados.

## 4.5. Comunicação e Gerenciamento de Operações

1. Os padrões de segurança da informação deverão estar à disposição de qualquer colaborador que requisitá-los. Os procedimentos deverão descrever, por escrito, como controles de segurança de informação eletrônica são autorizados, implementados e mantidos.

2. A implementação de novos sistemas ou atualizações maiores deverão observar a estratégia de Tecnologia da Informação da ASTRAZENECA e da COOPAZ. Novos sistemas e atualizações devem auxiliar e não ameaçar o progresso flexível e ágil de suporte a cooperados, permitindo que as aplicações estejam sempre prontas e acessíveis aos usuários autorizados.

3. O manuseio, reparo e descarte de equipamentos e mídia deverá observar um procedimento seguro e serviços autorizados. Para o correto descarte de informação eletrônica, os dados deverão ser apagados ou tornados ilegíveis (i.e., destruição de chaves de criptografia).

4. Procedimentos de manuseio e armazenamento de documentação de sistemas deverão ser criados para proteger estas informações de acessos não autorizados, vazamentos ou mal-uso. Documentação inclui, mas não se limita a processos de aplicação, procedimentos, configurações, estrutura de dados e autorização de processos, os quais deverão ser considerados.

5. Deverão ser mantidos procedimentos de back-up e restauração a fim de assegurar a confidencialidade, integridade e disponibilidade de informações e instalações de tratamento de informações em caso de desastre ou falha de sistema. Os procedimentos de back-up devem assegurar que todos os softwares e informações essenciais possam ser recuperados e os requisitos de organização da segurança da informação sejam satisfeitos.

6. Os requisitos de segurança da informação para confidencialidade, integridade e disponibilidade da informação eletrônica deverão ser considerados no back-up e nos processos de recuperação de desastres e de continuidade do negócio. Medidas de segurança deverão ser aplicadas em casos de recuperação de desastre e planos de continuidade do negócio que contenham informações sensíveis.

7. Conforme estabelecido em Lei ou em Convenções, deverão existir mecanismos para a comunicação organizada às autoridades competentes a respeito de incidentes de segurança significativos.

8. Dados e informações deverão ser mantidos por um prazo mínimo de 5 (cinco) anos, contados data em que foram adquiridos ou produzidos. Este prazo pode ser ampliado se assim determinado por Lei aplicável ou se necessário à finalidade do Tratamento, mas nunca reduzido, salvo em caso de alteração da Resolução BACEN nº 4.658, de 26 de abril de 2018.

9. A contratação de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem devem ser previamente comunicados ao BACEN, nos termos do artigo 15 da Resolução BACEN nº 4.658, de 26 de abril de 2018.

## 4.6. Procedimento de Identificação e Acesso

1. Controles de sistemas e redes de acesso baseados numa única identidade devem ser implementados, documentados e periodicamente revisados em observância aos requisitos do negócio. Controles de acesso deverão ser instalados para minimizar os riscos de vazamento de informações e permitir o perfeito e efetivo funcionamento das atividades da COOPAZ.

2. Um procedimento formal de cadastramento e descadastramento deverá ser implementado para garantir e revogar acesso a todos os sistemas de informação baseados e um único identificador. Estes procedimentos deverão prever controle de acesso de todos os registros de acesso.

3. Procedimento de Acesso de Usuário deverá ser instaurado para controlar a alocação de direito de acesso aos serviços e sistemas da informação. Os procedimentos deverão prever todos os estágios de cobertura do ciclo de vida do acesso do usuário, desde a subscrição de novos usuários até o cancelamento do cadastro de usuários que não mais terão acesso aos serviços e sistemas da informação.

## 4.7. Procedimento em caso de Incidente de Segurança da Informação

1. Todos os incidentes envolvendo Tecnologia da Informação e/ou falhas de segurança envolvendo informações críticas deverão ser reportados ao *Service Now* da AstraZeneca e ao responsável indicado da COOPAZ, assim que for descoberto o incidente.

2. Adicionalmente, deverá ser enviado para a COOPAZ, em até 3 (três) dias úteis, relatório contenho (a) identificação do incidente; (b) análise da causa, se conhecida; (c) impacto do incidente; e (d) medidas para controle do incidente.

3. Deverá ser designado dentro da Diretoria Administrativa um diretor responsável por elaborar relatório anual sobre a implementação do procedimento de resposta em caso de Incidente de Segurança da Informação, com data-base de 31 de dezembro, a ser apresentado à Diretoria Executiva até 31 de março do ano seguinte à data-base.

4. O relatório mencionado no tópico 3 acima deverá conter: a efetividade da implementação das ações do procedimento de resposta em caso de Incidente de Segurança da Informação, o resumo dos resultados obtidos na implementação das rotinas, dos procedimentos, dos controles e das tecnologias a serem utilizados na prevenção e na resposta a incidentes, os incidentes relevantes relacionados com o ambiente cibernético ocorridos no período; e os resultados dos testes de continuidade de

negócios, considerando cenários de indisponibilidade ocasionada por incidentes.

### 4.8. Compliance

A adequação dos sistemas de segurança da informação às políticas, padrões e procedimentos devem ser monitorados e reportados conforme escopo e frequência baseados no risco. Isso inclui o monitoramento da adequação por parte dos terceiros.

## 5. Glossário

| Termos | Definição |
|---|---|
| Administrador | Identifica um indivíduo que aprovou o serviço e é responsável por controlar a produção, desenvolvimento, manutenção, uso e segurança da informação e dos ativos. |
| Dispositivos | Unidade física de hardware incluindo, mas não limitado a: rede (network), dispositivos móveis (como smartphones, Computadores, tablets, iPads, mídia removível, tokens), aparelhos [internet das coisas (IOT)] que contém uma ou mais finalidades na computação. |
| Servidor | Serviços de Hardware ou Software que permitem o armazenamento lógico e a transmissão eletrônica de informações via internet, intranet e Extranet, incluindo Serviços de Software "SaaS" e serviços de armazenamento na Nuvem (Cloud). |
| Valor em risco da informação | A valoração do impacto no negócio no caso de vazamento de informações sensíveis. Incorpora a avaliação de impacto na confidencialidade, integridade e disponibilidade em casos de vazamento de dados. |
| Segurança Funcional de Tecnologia da Informação | Gerentes representantes de segurança e serviços de tecnologia da informação, não limitados a Arquitetos de Segurança e Seguranças de SMEs. |
| Método de transporte | Serviços de comunicações eletrônicas de aplicação com componentes e protocolos de segurança estruturados para fornecer comunicação segura de ponta a ponta (como e-mails, mensagem instantânea, Transferidor de Arquivos e Protocolos |

| | |
|---|---|
| | SFTP). |
| Classificação da Segurança da Informação | Baseado no Valor da Informação em risco, esta classificação é utilizada para determinar os controles apropriados e necessários para proteger informações eletrônicas. |
| Terceiro | Uma organização ou indivíduo que não é parte integrante da AstraZeneca, ou da COOPAZ, ou uma subsidiária da AstraZeneca. |

## 6. REFERÊNCIAS

| Ref ID | Nome do documento | Documento ID |
|---|---|---|
| 1 | AstraZeneca Global Policy: Corporate Information Technology Usage | LDMS_001_00161706 |
| 2 | IT standards (security and more) can be found:<br>AZ IT Policies & Standards<br>ITSEC standards, procedures and guidelines can be found:<br>Global IT Security site | |

## 7. HISTÓRICO DE REVISÃO

| Versão | Descrição da Atualização |
|---|---|
| 1.0 | Original |