





# ***CODE SECURITY***

**POLÍTICA DE SEGURANÇA**


	<b>POLÍTICA DE SEGURANÇA DA INFORMAÇÃO</b>	<b>PSI-001-2025</b>
		Versão: 1.0
	Classificação: Interna	Última revisão: 27/04/2025

## SUMÁRIO

<b>1. INTRODUÇÃO</b>	<b>4</b>
1.1. Objetivo	4
1.2. Escopo	4
<b>2. PRINCÍPIOS DE SEGURANÇA</b>	<b>5</b>
2.1. Confidencialidade	5
2.2. Integridade	5
2.3. Disponibilidade	5
<b>3. GERENCIAMENTO DE ACESSO</b>	<b>5</b>
3.1. Controle de Acesso	5
3.2. Autenticação	6
3.3. Autorização	6
<b>4. SEGURANÇA FÍSICA E AMBIENTAL</b>	<b>7</b>
4.1. Proteção de instalações	7
4.2. Controle de acesso físico	7
4.3. Segurança ambiental	7
<b>5. SEGURANÇA DE REDES E COMUNICAÇÕES</b>	<b>8</b>
5.1. Proteção de redes	8
5.2. Monitoramento e detecção de intrusões	8
5.3. Uso da internet	8
5.4. Uso do email corporativo	8
<b>6. GESTÃO DE INCIDENTES DE SEGURANÇA</b>	<b>9</b>
6.1. Resposta a incidentes	9
6.2. Relatórios de incidentes	9

 <b>CODE SECURITY</b>	<b>POLÍTICA DE SEGURANÇA DA INFORMAÇÃO</b>	<b>PSI-001-2025</b>
		Versão: 1.0
	Classificação: Interna	Última revisão: 27/04/2025

<b>7. CONSCIENTIZAÇÃO E TREINAMENTO EM SEGURANÇA</b>	<b>9</b>
<b>7.1. Programa de conscientização</b>	<b>9</b>
<b>7.2. Treinamento em segurança</b>	<b>10</b>
<b>8. AVALIAÇÃO E MELHORIA CONTÍNUA</b>	<b>10</b>
<b>8.1. Auditorias de segurança</b>	<b>10</b>
<b>8.2. Revisão de políticas e procedimentos</b>	<b>10</b>
<b>8.3. Análise de riscos</b>	<b>10</b>
<b>8.4. Medição de desempenho</b>	<b>11</b>
<b>9. CONFORMIDADE LEGAL E REGULATÓRIA</b>	<b>11</b>
<b>9.1. Conformidade com leis e regulamentações</b>	<b>11</b>
<b>9.2. Gerenciamento de vulnerabilidades e patches</b>	<b>11</b>
<b>10. RESPONSABILIDADES</b>	<b>12</b>
<b>10.1. Direção</b>	<b>12</b>
<b>10.2. Equipe de segurança da informação</b>	<b>12</b>
<b>10.3. Funcionários</b>	<b>12</b>
<b>11. DISPOSIÇÕES FINAIS</b>	<b>13</b>
<b>11. VIOLAÇÕES E PENALIDADES</b>	<b>13</b>
<b>12. DOCUMENTOS DE REFERÊNCIA</b>	<b>13</b>
<b>GLOSSÁRIO</b>	<b>14</b>

	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	PSI-001-2025
		Versão: 1.0
	Classificação: Interna	Última revisão: 27/04/2025

## 1. Introdução

### 1.1. Objetivo

A Code Security é integrante da administração indireta do Poder Executivo do Estado do Amazonas, e está vinculada à Secretaria de Estado da Agricultura. Tem por finalidade a execução das políticas públicas de recursos hídricos e irrigação do Estado, como o aproveitamento múltiplo da água, saneamento básico para comunidades rurais, estudos, pesquisas, ações de desenvolvimento social e econômico a partir do uso racional de águas subterrâneas, fluviais, reservamento de águas pluviais e irrigação no estado.


A segurança da informação é essencial para garantir a continuidade dos processos da Code Security, bem como proteger ativos de informação contra acessos não autorizados, alterações não autorizadas.

Esta política de segurança da informação define as diretrizes da Code Security para proteger a confidencialidade, integridade e disponibilidade das informações, cumprindo com as leis e boas práticas.

### 1.2. Escopo

Esta política se aplica a todos os funcionários, contratados, fornecedores e parceiros que lidam com as informações e ativos da organização.

- Redes internas e externas;
- Dados corporativos de clientes e parceiros;
- Dispositivos de comunicação.

 <b>CODE SECURITY</b>	<b>POLÍTICA DE SEGURANÇA DA INFORMAÇÃO</b>	<b>PSI-001-2025</b>
		Versão: 1.0
	Classificação: Interna	Última revisão: 27/04/2025

## 2. Princípios de Segurança

### 2.1. Confidencialidade

Garantir que a informação seja acessada somente por pessoas autorizadas.

### 2.2. Integridade

Assegurar a exatidão e a completude da informação.

### 2.3. Disponibilidade

Garantir que a informação esteja acessível quando necessário.

## 3. Gerenciamento de Acesso


### 3.1. Controle de Acesso

Para garantir que apenas pessoas autorizadas tenham acesso às informações da empresa, é fundamental estabelecer mecanismos de controles de acessos físicos e lógicos. Esses controles visam proteger os dados contra acessos indevidos e garantir que cada usuário tenha as devidas permissões necessárias para realizar suas atividades.

- Crachá de identificação;
- Senhas de acesso;
- Chave de segurança física.

As senhas devem conter no mínimo 8 caracteres, incluindo letras maiúsculas, minúsculas, números e símbolos. Devem ser trocadas a cada 60 dias e não devem ser anotadas e nem compartilhadas entre os funcionários.

O uso de dispositivos, credenciais ou senhas de identificação pertencentes a outra pessoa é estritamente proibido e constitui violação grave das políticas de segurança da organização.

	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	PSI-001-2025
		Versão: 1.0
	Classificação: Interna	Última revisão: 27/04/2025

Além das sanções internas cabíveis, tal conduta configura crime de falsa identidade, previsto no Código Penal Brasileiro, Artigo 307, que dispõe:

*"Atribuir-se ou atribuir a terceiro, falsamente, identidade diversa da própria, para obter vantagem, em proveito próprio ou alheio, ou para causar dano a outrem."*

Portanto, todos os colaboradores devem zelar pelo uso exclusivo e intransferível de suas credenciais, sob pena de responsabilização administrativa, civil e/ou criminal.

O acesso físico aos ambientes críticos será controlado por sistemas de autenticação (cartões, biometria, etc.).

**Visitantes devem ser sempre acompanhados.**

### 3.2. Autenticação


A autenticação é o processo utilizado para verificar a identidade dos usuários que possuem acesso aos sistemas da empresa. A Code Security adota alguns mecanismos de autenticação para garantir que apenas pessoas autorizadas possam acessar as informações.

- Utilização da autenticação multifator (**MFA**), combinado com outros fatores: senha e/ou biometria;
- Após múltiplas tentativas, ocorre o bloqueio automático do usuário ao sistema.

### 3.3. Autorização

A autorização define os níveis de permissão que cada usuário possui após ser autenticado no sistema. A code security trabalha com o princípio de menor privilégio, que garante que cada usuário tenha apenas os privilégios necessários para executar suas tarefas e nada mais.

- Os acessos aos dados sensíveis são restritos e monitorados;
- Alteração, exclusão ou inserção em perfis devem ser solicitados ao setor responsável da área.

	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	PSI-001-2025
		Versão: 1.0
	Classificação: Interna	Última revisão: 27/04/2025

## 4. Segurança Física e Ambiental

### 4.1. Proteção de instalações

O principal objetivo é evitar o acesso não autorizado nas dependências da organização. Isso inclui:

- Câmeras de Segurança;
- Portas com trancas;
- Salas dedicadas a servidores da organização.

### 4.2. Controle de acesso físico


Estabelecer medidas de controle de acesso para impedir o acesso não autorizado às áreas críticas.

- Crachá de identificação/acesso;
- Autenticação de múltiplos fatores (Fido).

### 4.3. Segurança ambiental

Implementar medidas para proteger os recursos de TI contra desastres naturais e outros riscos ambientais.

- Sistemas de detecção e combate a incêndios (Sensor de fumaça, extintores);
- CDP (Continuous Data Protection): Um backup quase em tempo real, cada vez que um dado é alterado, armazenando as informações na plataforma de nuvem utilizada pela organização;
- Defesa contra apagões (Nobreak, geradores de energia).

	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	PSI-001-2025
		Versão: 1.0
	Classificação: Interna	Última revisão: 27/04/2025

## 5. Segurança de Redes e Comunicações

### 5.1. Proteção de redes

A defesa de rede da empresa inclui a instalação de controles técnicos que minimizem os riscos de ameaças externas, como hackers e malwares, e internos como usuários mal intencionados.

- Utilização de Firewall para controle de tráfego de entrada e saída de dados;
- ACL (Lista de controle de acesso);
- Manter equipamentos de rede sempre atualizados.

É obrigatório o uso responsável e seguro da rede corporativa. Os usuários devem evitar o acesso a sites inseguros, downloads não autorizados e quaisquer atividades que possam comprometer a segurança da rede.

### 5.2. Monitoramento e detecção de intrusões

É essencial contar com mecanismos de monitoramento contínuo e detecção de atividades suspeitas na rede. Esses sistemas ajudam a identificar tentativas de intrusão, comportamentos indevidos e/ou violações de políticas, permitindo uma resposta rápida.

- Implantação de **IDS/IPS** (Sistemas de Detecção e Prevenção de Intrusões);
- Monitoramento de logs e eventos em tempo real;
- Definição de procedimentos claros para tratamento e resposta a incidentes;
- Retenção segura dos registros de auditoria para investigações futuras.


### 5.3. Uso da internet

O uso da rede que é fornecida pela Code Security é feita para atender ao propósito profissional, sendo a internet essencial para as atividades da nossa organização. Porém, o colaborador deve fazer uso da rede deliberadamente ciente das leis em vigor, respondendo pelo seu descumprimento.

### 5.4. Uso do email corporativo

O uso do email corporativo deve ser restrito somente nas dependências e sistemas da Code Security. Sendo de total responsabilidade do colaborador utilizar o correio eletrônico respeitando as regras de direitos autorais, licenciamento de software, direitos de propriedade e privacidade. A utilização de email pessoal é permitido apenas para o envio e recebimento de informações particulares.



	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	PSI-001-2025
		Versão: 1.0
	Classificação: Interna	Última revisão: 27/04/2025

## 6. Gestão de Incidentes de Segurança

### 6.1. Resposta a incidentes

A Code Security mantém um plano de resposta a incidentes que seguem as seguintes etapas:

- Identificação: Detectar e realizar registros de eventos suspeitos na rede ou dispositivos;
- Análise: É feita uma avaliação do evento para determinar se se trata de um acontecimento real e seu nível de gravidade;
- Realizar ação contra o evento: São tomadas medidas para cessar os impactos da “ameaça”;
- Remoção: Realizar a remoção da ameaça (Malware, user comprometido ou alguma vulnerabilidade);
- Restabelecimento: Fazer a restauração dos sistemas que foram afetados e realizar a normalização do sistema.

### 6.2. Relatórios de incidentes

Os funcionários ou terceiros que identificarem uma vulnerabilidade devem:

- Reportar a vulnerabilidade imediatamente ao time de Segurança, por meio de veículos oficiais como e-mail.


**O não reporte de vulnerabilidade pode comprometer o estado de segurança da empresa e está sujeito a medidas disciplinares.**

## 7. Conscientização e Treinamento em Segurança

### 7.1. Programa de conscientização

A Code Security desenvolveu um programa de conscientização em segurança para nossos apoiadores, com alguns objetivos como:

- Ter ampla compreensão dos funcionários sobre a importância da Segurança da Informação;

 <b>CODE SECURITY</b>	<b>POLÍTICA DE SEGURANÇA DA INFORMAÇÃO</b>	<b>PSI-001-2025</b>
		Versão: 1.0
	Classificação: Interna	Última revisão: 27/04/2025

- Estimular a cultura de realizar o reporte de comportamentos suspeitos a equipe responsável;
- Realizar alertas sobre os riscos cibernéticos muito comuns como o phishing e principalmente o uso inadequado de senhas.

## 7.2. Treinamento em segurança

A Code Security oferece treinamentos em segurança de forma obrigatória a todos os colaboradores, especialmente os funcionários que lidam com dados sensíveis.

- Novos funcionários passam por treinamento e ao longo dos vínculos com a empresa;
- Todas as capacitações são registradas para fins de futuras auditorias.

## 8. Avaliação e Melhoria Contínua

### 8.1. Auditorias de segurança

A Code Security está sempre preocupada em manter seus colaboradores cientes dos seus deveres em relação à segurança da organização. Portanto:

- Todo novo funcionário tem um treinamento envolvendo a política de segurança da empresa.
- São feitas auditorias anuais envolvendo conformidade, LGPD e a ISO 27002.


### 8.2. Revisão de políticas e procedimentos

- Para manter suas políticas de segurança em dia, a Code Security tem uma equipe dedicada para a atualização constante em relação às novas tecnologias e conformidade. Formada de:
  - Membros do setor de T.I
  - Membros do setor jurídico

### 8.3. Análise de riscos

Para estar sempre ciente de suas vulnerabilidades, ameaças que podem ser exploradas e quais seriam os impactos destes incidentes, a Code Security trabalha da seguinte maneira:

- Identifica os ativos, decidindo o que proteger;
- Identifica as ameaças;

	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	PSI-001-2025
		Versão: 1.0
	Classificação: Interna	Última revisão: 27/04/2025

- Identifica as vulnerabilidades;
- Avalia o risco utilizando a matriz de probabilidade x impacto.

#### 8.4. Medição de desempenho

Com o objetivo de seguir sempre em evolução, nossa organização mantém um programa constante para estabelecer os indicadores de desempenho, implementando:

- Auditorias e logs;
- Pesquisar internas;
- Avaliação do impacto do investimento em segurança.

### 9. Conformidade Legal e Regulatória

#### 9.1. Conformidade com leis e regulamentações

A Code Security acata um comportamento seguro no acesso aos dados dos seus colaboradores e clientes. Realizando:


- Correção e exclusão de dados;
- Registro do tratamento de dados;
- Minimizando a coleta de dados.

A Política de Segurança da Informação observa os preceitos legais previstos na legislação brasileira, incluindo, mas não se limitando à **Lei Geral de Proteção de Dados (LGPD)**, ao **Código Penal (Art. 307 – falsa identidade)** e demais normativas aplicáveis. Violações podem resultar em sanções administrativas, civis e criminais, conforme a gravidade do incidente.

#### 9.2. Gerenciamento de vulnerabilidades e patches

Sendo de grande importância sempre avaliar e corrigir suas vulnerabilidades, a Code Security aplica seus esforços da seguinte forma:

- Definindo responsáveis técnicos por redes e aplicações;
- Um cronograma quinzenal de varreduras e atualizações.

 <b>CODE SECURITY</b>	<b>POLÍTICA DE SEGURANÇA DA INFORMAÇÃO</b>	<b>PSI-001-2025</b>
		Versão: 1.0
	Classificação: Interna	Última revisão: 27/04/2025

## 10. Responsabilidades

### 10.1. Direção

A alta direção da Code Security, ciente das suas responsabilidades em relação a criação de regras e portarias, demonstra comprometimento com os seus colaboradores da seguinte maneira:

- Orientando constantemente seu pessoal quanto ao uso seguro dos ativos;
- Suporta as consequências da função e atividades ordenadas a outros colaboradores;
- Participar da investigação de incidentes de Segurança da Informação.

### 10.2. Equipe de segurança da informação


A equipe de Segurança da Informação da Code Security deve estar sempre atenta em relação aos seus deveres, que é proteger os ativos de informação contra ameaças internas e externas. Portanto, nossa equipe sempre presa:

- Trabalhar junto à equipe de infraestrutura e desenvolvimento;
- Trabalhar junto à equipe jurídica;
- Implementar atualizações nas políticas de segurança da informação;
- Monitorar e responder aos incidentes.

### 10.3. Funcionários

Assim como a direção, os funcionários desta organização devem estar cientes dos seus deveres envolvendo a segurança da Code Security. Podendo exercer esse dever da seguinte forma:

- Ser cauteloso em relação às informações expostas da sua função e atividades dentro da organização;
- Participar de reuniões sobre a Segurança da Informação, caso convocado;
- Reportar incidentes que possam impactar a segurança da Code Security.

 <b>CODE SECURITY</b>	<b>POLÍTICA DE SEGURANÇA DA INFORMAÇÃO</b>	<b>PSI-001-2025</b>
		Versão: 1.0
	Classificação: Interna	Última revisão: 27/04/2025

## 11. Disposições finais

O presente documento deve ser lido e interpretado sob a égide das leis brasileiras, no idioma português, em conjunto com outras normas e procedimentos aplicáveis pela Code Security e mantidas.

Quaisquer atitudes ou ações indevidas, ilícitas, não autorizadas ou contrárias ao recomendado por esta Política ou pelas demais normas e procedimentos de segurança da informação da Code Security serão considerados violações por si só e estarão sujeitas às sanções previstas no Regimento Geral, contratos de prestação de serviços, contratos de trabalho e nas demais normas da instituição.

Os casos de incidente, infração ou suspeita dessas ocorrências deverão ser comunicados imediatamente.


### 11.1. Violações e Penalidades

O descumprimento das diretrizes estabelecidas nesta política poderá acarretar sanções que variam desde advertência formal até desligamento por justa causa, conforme o caso. Também poderão ser aplicadas medidas legais cabíveis. Todas as infrações serão analisadas pela equipe de Segurança da Informação em conjunto com o setor jurídico.

## 12. Documentos de referência

O presente documento está em conformidade com os seguintes documentos:

- BRASIL. Lei Geral de Proteção de Dados Pessoais. Lei nº 13.709, de 14 de agosto de 2018;
- BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil;
- ABNT NBR ISO/IEC 27001:2013 – Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Requisitos;
- ABNT NBR ISO/IEC 27002:2013 – Tecnologia da informação — Técnicas de segurança — Código de prática para controles de segurança da informação.

	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	PSI-001-2025
		Versão: 1.0
	Classificação: Interna	Última revisão: 27/04/2025

## GLOSSÁRIO

**PSI (Política de Segurança da Informação):** Documento que define as diretrizes e normas de proteção da informação da organização.

**MFA (Multi-Factor Authentication):** Método de autenticação que exige dois ou mais fatores distintos para validar a identidade do usuário.

**ACL (Access Control List):** Lista de Controle de Acesso utilizada para definir permissões de acesso em redes e sistemas.

**CDP (Continuous Data Protection):** Proteção Contínua de Dados que realiza backups quase em tempo real, salvando alterações automaticamente.

**IDS (Intrusion Detection System):** Sistema de Detecção de Intrusões que monitora redes para identificar comportamentos suspeitos.

**IPS (Intrusion Prevention System):** Sistema de Prevenção de Intrusões que detecta e bloqueia atividades maliciosas em redes.


**TI (Tecnologia da Informação):** Área responsável pela gestão de tecnologias, redes, sistemas e dados da organização.

**LGPD (Lei Geral de Proteção de Dados Pessoais):** Lei brasileira que regulamenta o tratamento de dados pessoais e estabelece direitos e deveres sobre sua proteção.

**Confidencialidade:** Garantir que a informação seja acessada somente por pessoas autorizadas.

**Integridade:** Assegurar a exatidão e a completude da informação, prevenindo alterações não autorizadas.

**Disponibilidade:** Garantir que a informação esteja acessível para uso sempre que necessário.

	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	PSI-001-2025
		Versão: 1.0
	Classificação: Interna	Última revisão: 27/04/2025

**Controle de Acesso:** Mecanismos implementados para assegurar que apenas usuários autorizados possam acessar recursos físicos ou digitais.

**Autenticação:** Processo para verificar a identidade de usuários que acessam sistemas ou ambientes.

**Autorização:** Definição dos níveis de permissão de usuários autenticados para acesso a informações e recursos.

**Firewall:** Ferramenta utilizada para filtrar e proteger o tráfego de dados de redes.

**Gerenciamento de Vulnerabilidades:** Processo de identificar, avaliar e corrigir falhas de segurança em redes, sistemas e aplicações.

**Patch de Segurança:** Atualização de software aplicada para corrigir vulnerabilidades ou falhas de segurança.


**Análise de Riscos:** Processo de identificar, avaliar e tratar ameaças e vulnerabilidades que possam impactar a organização.

**Backup:** Cópia de segurança de dados feita para garantir sua recuperação em caso de falha ou perda.

**Logs:** Registros de eventos e atividades gerados por sistemas e redes para auditorias e investigações.

**Auditoria de Segurança:** Avaliação sistemática dos processos, práticas e controles de segurança da informação.

**Resposta a Incidentes:** Conjunto de ações adotadas para identificar, conter, erradicar e recuperar-se de incidentes de segurança da informação.

 <b>CODE SECURITY</b>	<b>POLÍTICA DE SEGURANÇA DA INFORMAÇÃO</b>	<b>PSI-001-2025</b>
		Versão: 1.0
	Classificação: Interna	Última revisão: 27/04/2025

**Relatório de Incidentes:** Documento ou comunicação formal utilizado para reportar vulnerabilidades ou incidentes de segurança detectados.

**Programa de Conscientização:** Conjunto de ações educacionais para promover o conhecimento sobre segurança da informação entre os colaboradores.

**Treinamento em Segurança:** Capacitação obrigatória oferecida aos colaboradores para garantir o entendimento e a prática das normas de segurança.